MIST

Maritime Information Sharing Taskforce

Ports of Delaware Bay

Industry and Public Sector Cooperation for Information Sharing

Anita Salem
Wendy Walsh
Lyla Englehorn

December 2010

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
DEC 2010

2. REPORT TYPE

3. DATES COVERED
00-00-2010 to 00-00-2010

4. TITLE AND SUBTITLE
Industry And Public Sector Cooperation For Information Sharing: Ports Of Delaware Bay

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School, Operations Research Dept,Monterey,CA,93943

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Maritime Information Sharing Taskforce (MIST) is an interagency research effort to capture best practices in information sharing in a regional port environment. MIST creates a structure for collaborative problem solving that focuses on uncovering unique local issues and communicating these to national policy makers. The MIST team is led by the Maritime Defense and Security Research Program (MDSRP) at the Naval Postgraduate School (NPS) in partnership with several federal agencies including the Department of Transportation?s Maritime Administration (MARAD), the Office of the Director of National Intelligence?s Global Maritime and Air Intelligence Integration (GMAII) and the National Maritime Domain Awareness Coordination Office (NMCO).

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**57**	

TABLE OF CONTENTS

MIST Delaware Bay Highlights

The Maritime Information Sharing Taskforce (MIST) held its fourth event in Philadelphia on September 28-29, 2010. Using a participatory design approach, NPS researchers partnered with federal, state, local and commercial stakeholders to conduct a process to assess the information sharing needs of security personnel in this port region.

Key Findings

Incentives should match local motivations. Similar to our other sites, Philadelphia called for operational and financial incentives for information sharing: quicker business resumption after an event, protection of assets, and fewer costs incurred. In addition, this port emphasized improving their strategic positioning by generating positive public opinion and being seen as environmental stewards. A key cultural differentiator for Delaware Bay was their ethos of team work and a pride in their ports: "It's all about the love in Philadelphia." It's also about how they work together: "We have a common interest in making things better."

Streamlining government is important because operational efficiencies save the private sector money, improve a company's reputation and result in greater customer satisfaction. Areas that the participants targeted for improvement include more effective communication and simpler processes**.** The lack of communication makes them feel left out of the loop: "Maybe I'd have done things differently had I known—I'd have been more alert." Government participants noted these difficulties and saw their world becoming even more complex due to new legislation and new technologies: "It's a patchwork."

Threat Information needs to be readily accessible and relevant. Participants want easy access to threat information and need to be able to have some access to classified information. Industry needs information that is relevant, consistent, and actionable: "We get Intel information that we have no idea what to do with." Finally, when using Homeport, participants found it only somewhat desirable and useful. The site was slow loading and was missing or had outdated information. This frustrated the participants and made them question the credibility of the information.

Successful local models for information sharing can help other ports learn best practices. Delaware Bays' best practices included the AMSC, four state fusion centers, and private sector associations. The AMSC is a primary source of information and networking. The fusion centers' mission is to analyze and disseminate all hazards information, and the new Delaware Valley Intelligence Center (DVIC) will incorporate private sector input. The Maritime Exchange assists with daily vessel schedules, alerts, statistics and training. When evaluating these models, participants stressed the importance of having broad participation by intermodal partners, methods to encourage consistent attendance, and procedures for sharing of sensitive information.

Recommendations for government action

1. Address the process for issuing clearances
2. Expand maritime and intermodal information sharing
3. Create a feedback system for keeping industry in touch
4. Increase industry awareness of crew repatriation and suspicious activity
5. Increase consistent attendance of AMSC
6. Increase the number of coordinated exercises
7. Utilize VIPR teams more broadly
8. Align federal efforts, especially DVIC and NMIC
9. Support sustainability of information sharing
10. Create an action plan for moving forward

Recommendations for local action

11. Expand Maritime Familiarization Day and agency training exchange program
12. Identify and document shared resources
13. Improve communication with the trucking industry
14. Advertise training opportunities

MIST

The Maritime Information Sharing Taskforce (MIST) is a two-way process for understanding and communicating the needs of local, private sector communities when sharing maritime threat information. Our goals are to:

- Capture best practices in information sharing
- Create a structure for collaborative problem solving
- Convey unique local issues to national policy makers

MIST is led by the Maritime Defense and Security Research Program (MDSRP) at the Naval Postgraduate School (NPS) and was established in the fall of 2008. The MIST process consists of a series of local events held at individual ports across the United States. Each local event builds upon lessons learned from earlier events and invites participants to join in on the design of the event.

MIST Sites

- Los Angeles/Long Beach, CA
- Puget Sound region
- Honolulu, HI
- Delaware Bay region

Federal partners

- DOT-MARAD
- GMAII
- NMCO
- ISE
- DHS-USCG, CBP, TSA
- FBI/DOJ
- DoD-MDA EA, DON & ASD-HD/ASA

Introduction

The Maritime Information Sharing Taskforce (MIST) is an interagency research effort to capture best practices in information sharing in a regional port environment. MIST creates a structure for collaborative problem solving that focuses on uncovering unique local issues and communicating these to national policy makers. The MIST team is led by the Maritime Defense and Security Research Program (MDSRP) at the Naval Postgraduate School (NPS) in partnership with several federal agencies including the Department of Transportation's Maritime Administration (MARAD), the Office of the Director of National Intelligence's Global Maritime and Air Intelligence Integration (GMAII) and the National Maritime Domain Awareness Coordination Office (NMCO).

MIST is foremost a process. It consists of a series of activities and local events held at individual ports across the United States. Each MIST process builds upon lessons learned from earlier events and invites participants to submit input on the design of each event. A local MIST process consists of five core activities designed to help surface maritime domain awareness (MDA) issues that are important to private sector shipping. The core activities encompass the following elements:

1. ***Community Bridging***

   The research team stresses active local participation. We first study the regional port environment to identify key players and business activities. We then talk with the key players and uncover the local challenges and best practices in information sharing. The lead program manager then typically presents the MIST process to the local Area Maritime Security Committee (AMSC) and convenes a local steering committee to provide direction, build buy-in and aid in recruitment.
2. ***Social Networking***

   A primary goal of the MIST process is to build an environment where the participants can freely share information. We offer polls to allow participants to surface topic issues and priorities prior to the workshop. We utilize a local steering committee to reach out to potential participants. And finally, we collect local contact and training information that can be used internally and by other agencies.
3. ***Information Flow***

   An important goal of the MIST process is to get a realistic sense of information flow in a specific port environment. In support of this, the research team engages in a role specific field study. This field study follows an operator in their daily work and interviews the participant to gain a greater understanding of their perspective on the sharing of information between industry and government stakeholders. The studies include the perspectives of field and vessel security officers and are conveyed in sidebars within the full report.
4. ***Local Issues***

   The workshop is the most in-depth element of the process and it is focused on local issues in information sharing. It is a day and a half workshop with approximately 30 information sharing stakeholders within a specific region. There is a distinct effort to ensure a variety of industry and government stakeholders. The researchers conduct small and large group activities to surface real world challenges in collaboration and identify incentives for information sharing. The workshop closes with the identification of next steps and recommended actions on specific issues in information sharing.
5. ***Communication***

   At the end of each MIST event, we create a detailed report on our findings in a regional specific MIST report. This report is widely socialized by the MIST research team through meetings, briefs, conference presentations, articles and blogs. The report itself is expected to be employed as an investment justification for port security grants to highlight information sharing priorities and efforts underway.

The fourth MIST workshop was held in Philadelphia, Pennsylvania on September 28-29, 2010. Previous MIST events have been held at the Port of Los Angeles/Long Beach, the Ports of the Puget Sound with a workshop in Seattle, and the Port of Honolulu in Hawaii. The goal for each event is to provide a venue for private sector input to the development of information sharing processes.

MIST Delaware Bay

Delaware Bay is unique in that three states share the shoreline of the Delaware River and Bay – Delaware, New Jersey, and Pennsylvania; in addition, Maryland is included in many cross jurisdictional plans and efforts. Most other major seaports are completely within the jurisdiction of a single state. In Delaware Bay twelve counties, five public port authorities, and many municipalities all share responsibility for and have a significant stake in the management of the region. With the construction of a 40 foot deep canal in the upper river in the 1960s, the Delaware Bay accommodates deep draft navigation from the Delaware Capes inland 130 miles to Morristown, PA. The Delaware River Port of Philadelphia is one of the oldest operational seaports in the U.S.[1]

The MIST Delaware Bay process began in August 2010 with an initial outreach to the Delaware Bay AMSC, an introductory field study, and pre-workshop polling. For the field study, researchers spent time with selected industry members and recorded real time, on site observations about the work environment and information sharing practices in the Delaware Bay region. In advance of the workshop, we polled confirmed participants about their top concerns and issues with information sharing in the maritime environment. Finally, at the end of September, the MIST team facilitated a day and a half workshop graciously hosted by the U.S. Coast Guard (USCG) Sector Delaware Bay in their Philadelphia headquarters building.

The MIST Delaware Bay process included stakeholders from all four states, and from all levels of government, law enforcement, and industry. We also included intermodal partners and representatives from regional fusion centers. These intermodal and fusion center partners play an important role in the sharing of maritime security information.

Intermodal Information Sharing

Based on stakeholder input, the MIST team for the first time targeted intermodal information sharing for discussion. As passenger traffic and volume of commerce continue to increase under the pressure of globalization, information sharing between intermodal stakeholders is essential to homeland and global security efforts.[2] In May 2007 the Transportation Security Administration (TSA) released the Transportation Systems Sector-Specific Plan (TSSP), and defined the six primary national transportation modes: aviation, maritime, mass transit highway, freight rail, and pipeline.[3] Although these modes each operate independently, they are also highly interdependent based on what is needed to move the resource. (For example, aviation fuel, though used in one mode is transported over pipelines, trucked in on highways, and moved by barge and ship.) The U.S intermodal transportation network, which moves millions of passengers and significant volumes of

[1] Ives, 1997

[2] GAO Report: 10-435R, 2010

[3] TSA TSSP, 2007

essential goods each year, is a vast and open network involving a plethora of stakeholders across all levels of government and industry and is a challenge to secure [4] .

Disruptions to the U.S. intermodal transportation system have significant ramifications for national and global security and economic well-being. Potential disruptions to the transportation system sector include natural disasters, accidents, and terrorist attacks. Recent events demonstrate the significance of intermodal information sharing: in New York and Washington, DC, on September 11, 2001, and later in London, Madrid, and Mumbai, intermodal transportation was used as part of a terrorist attack.[5] The vastness of the intermodal transportation network—18 industry sectors, six transport modes, and 4 million miles of road—present enormous cultural, technological and operational challenges to information sharing.[6] As a result of this complexity, intermodal information sharing efforts have been varied in their approach and their breadth of involvement. A recent GAO report concluded that although several federal level agencies are supporting the establishment of intermodal information sharing entities, these efforts continue to face operational and management challenges.[7]

Several intermodal efforts have a demonstrated a history of success and a potential for continued improvement. One example of successful intermodal information sharing is the preparation, response, and recovery of Critical Infrastructure and Key Resource (CI/KR) sectors after the Midwest flooding and Gulf Coast hurricanes of 2008.[8] Another example is the TSA's Visible Intermodal Prevention and Response (VIPR) security teams.[9] These teams serve as a kind of force multiplier for transit agency security efforts. They enhance security resources during special events and are often deployed at mass transit locations.[10] Between December 2005 and August 2007, VIPR teams were deployed over fifty times.[11] Future plans include expansion of VIPR team efforts to other intermodal locations and facilities and as a start, the Philadelphia MIST event included local VIPR team participation.

Funding opportunities for intermodal efforts have also increased. To support transportation infrastructure and security, DHS has recently allocated funds to state and local jurisdictions through the American Recovery and Reinvestment Act (ARRA). Of the total funds, $14.5 million was allotted to the Freight Rail Security Grant Program to protect freight rail systems infrastructure from acts of terrorism, specifically railroad cars transporting toxic inhalation hazardous materials. Through the Transit Security Grant Program, another $403 million was awarded to protect critical transit infrastructure, and to complete much needed capital projects, such as improvements to high-risk,

[4] It is important to note that as much as eighty-five percent of the intermodal transportation infrastructure in the United States owned by the private sector (TSA TSSP, 2007)

[5] TSA TSSP, 2007

[6] 18 Industry Sectors: Agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, information technology, national monuments and icons, nuclear, postal and shipping, public health and healthcare, transportation, and water (GAO, 2010)

[7] GAO-10-435R, 2010

[8] Hughes, 2009

[9] VIPR teams consist of a combination of Surface Transportation Security Inspection agents, Federal Air Marshals, explosive-detection canine teams, Aviation Security Inspectors, and Transportation Security Officers (TSA, August 2007)

[10] VIPR deployment locations include the Massachusetts Bay Transportation Authority (MBTA) system in Boston, at Amtrak facilities in Boston, upstate New York, Philadelphia and Washington DC, and at the Niagara Frontier Transportation Authority and Amtrak facilities in Buffalo, New York (TSA, August 2007)

[11] TSA, August 2007

high-density tunnels, stations, and bridges. Another $20 million was provided for intercity passenger rail to protect infrastructure and the traveling public.[12] This commitment of funds at a time of shrinking budgets demonstrates the essential role freight and passenger rail play in U.S. safety and security. It will be critical to ensure these projects work in concert with other efforts to address the interdependent intermodal nature of transportation and maximize the effectiveness and efficiency of any proposed solutions.

Finally, other existing programs are being expanded to intermodal. For instance, the U.S. Department of Homeland Security (DHS) Suspicious Activity Reporting (SAR) initiative is going intermodal. During a whistle-stop train tour in July 2010, DHS Secretary Janet Napolitano announced a new national information-sharing partnership with Amtrak as part of the Department's nationwide SAR initiative. This new national information-sharing partnership will allow DHS and the Department of Justice (DOJ) to work with Amtrak using the latest intelligence techniques to identify suspicious behaviors associated with new and evolving threats. The Suspicious Activity Reporting Initiative establishes a unified approach at all levels of government to gather, document, process, analyze, and most importantly share information about terrorism-related suspicious activities.[13] The Amtrak SAR effort is one of the first steps toward implementing this level of information sharing with regional railways, freight rail carriers and other mass transit agencies.

Fusion centers & the DVIC

Although law enforcement has participated in prior MIST efforts, the fusion center representation at this event added a new richness to this workshop. Fusion centers and information sharing have been the focus of many efforts across the federal landscape since the 9/11 terrorist attacks. In May 2010, President Obama issued his National Security Strategy, which among other things, reinforced the "whole of government" approach to information sharing. This approach is based on the central concepts of open government—transparency, participation, and collaboration. Collaboration with private sector partners is particularly emphasized in the strategy:

> *"The ideas, values, energy, creativity, and resilience of our citizens are America's greatest resource. We will support the development of prepared, vigilant, and engaged communities and underscore that our citizens are the heart of a resilient country. And we must tap the ingenuity outside government through strategic partnerships with the private sector, nongovernmental organizations, foundations, and community-based organizations. Such partnerships are critical to U.S. success at home and abroad, and we will support them through enhanced opportunities for engagement, coordination, transparency, and information sharing"*[14]

Facilitating information sharing is the primary responsibility of the seventy plus fusion centers distributed throughout the nation. Fusion in this effort is defined as "the overarching process of managing the flow of information and intelligence across all levels and sectors of government and

[12] DHS, November 2010
[13] John O'Connor (DHS, July 2010)
[14] National Security Strategy, May 2010

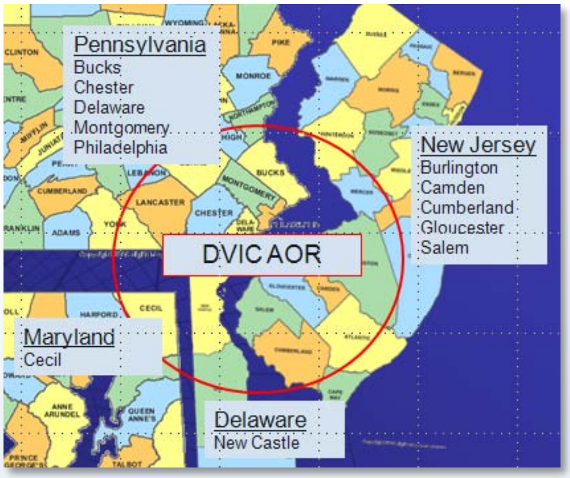
private industry."[15] In practice, the fusion process transforms information from disparate sources into actionable knowledge – a process sometimes termed sense-making. Fusion centers "bring together law enforcement, public safety agencies, and private sector partners to increase their ability to detect, prevent, investigate, and respond to criminal and terrorist activity".[16] Primary to the fusion center mission is the collection, integration, evaluation, analysis and dissemination of information.

Recognizing the need for such an effort in the geographically unique Delaware Valley region, the Delaware Valley Intelligence Center (DVIC) was initially proposed in March 2005. After a series of meetings over the next two years the concept matured, and a contractor was selected in December 2007 to perform an Implementation Assessment and Cost Analysis. A location has been secured, and the DVIC will be operational in approximately nine months. Unlike other fusion centers that serve an area defined by state boundaries, the DVIC will serve an area that includes twelve counties in four states that all share shoreline on the Delaware River and Bay. Located in Philadelphia, the DVIC will leverage the capabilities of existing state fusion centers, federal agencies, regional taskforces, and private sector partners. Based on careful, thoughtful, and thorough planning the DVIC effort strives to be a model of the "whole of government" approach essential to successful information sharing.

Spotlight: The Delaware Valley Intelligence Center

SOURCE: DIVC presentation, September 2010

The *DELAWARE VALLEY INTELLIGENCE CENTER* (DVIC) is essentially a broad fusion of fusion centers in the Delaware Valley Region, and will serve as 24/7information sharing support for All Crimes and All Hazards in the four state Delaware Valley region. The DIVC will support tactical and business operations, investigation and intelligence gathering, strategic planning and budget processes. The DVIC will link regional field assets, enhance situational awareness and serve as a continuity of operations resource for regional partners. The DVIC has a rich structure of organizational collaboration that spans Federal, State, Local and Tribal entities including law enforcement, fire, social services, healthcare, transportation, commerce, all DHS critical infrastructure domains, education and non-governmental organizations. Unique to the DVIC is the level of private sector participation and a significant maritime focus. The planning for the DVIC is a model and will certainly ensure successful implementation.



Timeline

- 2005 – Vision to establish shared Intel
- 2006 – Outreach to DHS
- FEB 2007 – Grant funding
- DEC 2008 – Vendor selection
- NOV 2009 – Phase I complete
- 9-1-2010 – Phase II approval to proceed
- 9-7-2010 – DHS Intel Analyst assigned to DVIC
- NOV 2010 – Facility lease, implementation
- JAN 2011 – Phase II refinements complete
- 1-31-2011 – Activate DVIC cell
- SEPT 2011 – Philadelphia PD assets into DVIC

DVIC Partners

ATF
DE OHS
FBI
NJ OHSP
Utilities
Pa State Police
Phil. Police
Public Health

Business
DE State Police
FEMA
NJ Police/EM
PA OAG
PARTSWG
Phila-Camden HIDTA
SEPA RTF

Figure 1: The DVIC

[15] Fusion Center Guidelines, August 2006

[16] Global Justice Information Sharing Initiative, April 2008

Discussion of Findings

The fourth MIST event was held in Philadelphia, Pennsylvania on September 28-29, 2010. Previous MIST events were held at the Port of Los Angeles/Long Beach, the Ports of the Puget Sound, and the Port of Honolulu. Our goal for MIST events is to provide a venue for private sector input to the development of information sharing processes.

To support our goals, we conducted a field study with FSOs and facilitated a day and a half workshop with selected port personnel. The field study data that we collected was analyzed for high level trends (*see sidebars on page 9 and 12*).

During our work in Delaware Bay, we explored six areas related to information sharing:

- Incentives
- Measures of effectiveness
- Government processes
- Information & communication
- Trust & Culture
- Models for information sharing

This section presents a high level view and discussion of the findings. Complete details on our findings can be found in the full report.

Incentives

Participants from the Delaware Bay identified a number of incentives for sharing threat information. This port had a well balanced set of desired benefits, emphasizing financial, operational, and social incentives in their top five incentives.

1. Quicker business resumption after an event
2. Protection of assets
3. Positive public opinion
4. Environmental stewardship
5. Fewer costs incurred

Of particular note is the fact that private sector participants viewed quicker business resumption, fewer costs incurred, and increased port use higher than government participants. This difference in perception may impact how government representatives approach information sharing.

Following is a discussion of specific incentives identified as desirable by Delaware Bay.

Operational and strategic benefits

"If you know what to expect, you may make better decisions and plans"

Delaware Bay participants indicated that operational and strategic benefits were an important motivator for participating in port

Spotlight: About FSOs

(Facility Security Officers)

Nationally, we are seeing three types of facility security officers (FSOs). At previous ports, the dominant facility security profile was the security officer who came up through the operations side of the house. At the ports of the Delaware Bay region however, 3 of 3 FSOs had strong backgrounds in law enforcement.

The law enforcement FSO

These FSO's are focused primarily on improving their company's security operations. They have spent a good part of their career in local police or federal law enforcement agencies and come with a lot of skill and respect for good security. Often, they do not have backgrounds in the maritime industry and need to learn more about maritime operations to function well in their role.

The former Coast Guard FSO

FSOs coming from the U.S. Coast Guard (USCG) are highly aware of federal safety and Homeland security issues. They are often retired from the Coast Guard in the local area and leverage their USCG connections and knowledge to improve their company's policies and procedures. They are usually well versed in the maritime environment and processes but have an initial learning curve in understanding private sector operations and culture.

The safety officer FSO

Many of the FSOs that we have studied have grown up in maritime port operations and have only gotten involved in security since 2004. With their diverse backgrounds in port operations, they are often tasked with multiple responsibilities. They have taken training with the USCG to help them develop security plans and processes. However, they are focused on safety first and security second.

security operations. Participants discussed how both operational efficiencies and improved strategic position improved their business operations. Greater efficiency leads to increased productivity, which leads to lower costs, builds a reputation for being cost effective and results in higher customer satisfaction. Participants noted how information sharing helps both strategically and operationally: "If information is shared with the right people at the right time, we are more effective."

Social and Ideological benefits

"Many hands make light work… sharing can result in increased awareness for all."

In Delaware Bay, participants expressed pride in their ports and in their relationships. They see themselves as team players who want to make things better rather than pointing out what doesn't work. Trust is an important part of their ethos and they identified teamwork as an important factor that helps build trust: "To feel a part of an organization, to have a say…to be part of a team" is important in their work. As team players, their focus is on making things better and holding each other accountable. This includes making the ports safer, being environmentally healthy, and increasing workplace satisfaction.

Financial benefits

"We're in the business of making money"

The Delaware Bay participants generally agreed that financial benefits were a very important incentive for information sharing. Attracting and retaining business, maintaining a resilient community, and ensuring business continuity were all important factors. The participants also noted how both operational efficiencies and environmental concerns were related to financial benefits. Operational improvements mean less time, and less time means more money. Environmentally, lower fuel use resulting from fast turnaround times not only improves the environment but also means less fuel burned, resulting in cost savings. Financial benefits were often the end result of other perceived benefits and were an important factor in their decision making.

Recommendations for aligning incentives

1. Support and join in on local team building efforts
2. Train new government personnel in local cultural behaviors (e.g. expand existing agency education programs)
3. Provide threat information that helps the private sector allocate resources appropriately

Measures of effectiveness

As part of our effort to identify key factors in information sharing, we look for ways that we can measure the success of information sharing efforts. These measures of effectiveness allow us to assess the impact of specific initiatives and see if our efforts are leading to desired results. In each port, participants have identified effect measures that are important. Although not probed directly, participants from the Ports of Delaware Bay added an additional item (speed of access to information) to our list of measures of effectiveness for information sharing, bringing the total to 14 items covering four areas:

- Ease of access to information
- Operational efficiency
- Response capability
- Preparedness capability

Challenges with streamlining government interactions

"We have no information when a threat is suspected…"

In their day to day lives, port personnel can deal with a handful of industry organizations, a dozen or so state and local agencies, and almost two dozen federal and international agencies. For our participants, the two most important agencies were the USCG and the CBP. When it comes to information sharing, Delaware Bay participants called first for more effective reporting and communication processes, and secondly for simpler processes. Specific issues that participants identified included:

- Lack of centralized systems for communication
- Inadequate coordination of policies (e.g. crew pick up, crew repatriation, TWIC[17])
- Inadequate coordination with trucking and rail
- Unrealistic expectations
- Unrealistic risk assessments

Participants identified several agencies and activities that showed a well coordinated response:

- GPS and Hazmat tracking
- DOT-PHMSA pipeline sensors
- DoD and the coordination of fuel movements
- FBI's WMD coordination
- U.S. Federal Marshal's VIPR teams
- Intelligence products from the DVIC

Recommendations for streamlining

4. Provide a central source for getting threat information
5. Place a stronger emphasis on team building with the private sector through cross cultural training, exercises, and more face-to-face interactions
6. Increase collaboration with the USCG, CBP, trucking, and rail
7. Include the private sector more when planning exercises
8. Include the private sector in planning for the DVIC
9. Improve the crew repatriation process

[17] a Transportation Security Administration and U.S. Coast Guard initiative, the Transportation Worker Identification Credential (TWIC) program provides a tamper-resistant biometric credential to maritime workers requiring unescorted access to secure areas of port facilities, outer continental shelf facilities, and vessels regulated under the Maritime Transportation Security Act of 2002 (MTSA), and all U.S. Coast Guard credentialed merchant mariners.

Challenges with information flow

"I want information I can take and do something with not broad educational information."

An important outcome for MIST is to uncover private sector needs in regards to the sharing of threat information. To support this outcome, we conducted field studies of Facility Security Officers (*see sidebars on page 9 and 12*), held workshop discussions on the topic, and had participants work with a local Homeport site. The results show that our participants want streamlined access to threat information and actionable information and tools.

Improve access to information

"We have no information when a threat is suspected until they show up and then the ship can't move and it's costing us money."

A key barrier to information sharing is getting access to the information. Participants complained that often they did not receive the information they needed: "It's unfortunate…we have no information when a threat is suspected"
Delaware Bay participants, like their counterparts at other ports, want a central repository for information and requirements, want easy access to threat information and need to be able to have some access to classified information. In addition, these participants noted the importance of providing on-going feedback to people in the field: "There is nothing more satisfying than calling and telling that the case is closed—we need to respond to those that report otherwise they will stop reporting." The participants noted that improvements need to be made in sharing information systematically, utilizing existing systems, and communicating more effectively. Barriers to providing information include legal ramifications, the risk of incorrect information, internal pressures, lack of resources and insufficient trust.

Improve the quality of information and tools

"We get Intel information that we have no idea what to do with…give us actionable information"

To uncover specific issues with information quality we conducted an informal poll and a scenario using Homeport. Participants identified the need for information that is relevant, consistent, and easy to use. Useful information is information that is specific and actionable, is consistent, and includes follow-ups. Relevant information is information that is actionable: "I want information I can take and do something with rather than broad educational information." Consistency in how information is presented is also important because it leads to increased ease of use and increased trust in the reliability of the data.

Spotlight: What do FSO's need?

FSO's need to do security cheaply.

"I'm doing a balancing act between the economic downturn and what we need to do as far as implementing all the requirements"

All FSOs are challenged with justifying their efforts based on the cost and the impact on operations. The FSO with law enforcement background in the Delaware Bay region is (over)tasked with a wide variety of security activities:

- managing TWIC
- monitoring access
- researching security patterns
- documenting and coordinating security activities, grants, contracts, and security plans
- participating in local and national planning and investigations

FSO's need help with requirements.

"If you are going to put these kinds of requirements on me, then give me a way to meet your requirement standards."

They need:

- realistic standards
- an understanding of their world
- minimal political maneuvering
- a clear return on their investment

FSO's need effective communication

"The government is a collector of information, they don't give you any."

FSO's at the Port of Delaware Bay interact with people in a variety of ways:

- **Information sharing** is often face-to-face but also electronic: siren announcements, radios, phones, email, and Blackberry's.
- **Incident reporting** is to the USCG, NRC, DIAC, and 911 Centers.
- **Sharing of threat information** is primarily with Port tenants, the FBI, and the EPA.
- **Exercises** often involve all four states, the federal government, and the private sector.
- **Daily communication** is with the TSA, USDA, and the CBP.
- **Weekly communications** occurs with local law enforcement

Improve the usability of Homeport

"The page is empty…maybe there's no threat"

Homeport is the official Coast Guard information technology system for maritime security created to provide information and services to the maritime community and the public over the Internet. It is designed to support the sharing, collection and dissemination of sensitive but unclassified information to targeted groups of registered users within the port community. During the workshop, we had the participants use the web site to locate specific threat information. Overall, participants had difficulty using the site and found it only somewhat desirable and useful. Useful features included alerts and notifications and the ability to link all sectors. However, users found the site somewhat difficult to use resulting in frustration and perceptions that the site was not credible or useful. User difficulties included slow load speeds, outdated or non existing information, and difficult navigation.

Consider other information sources

"Consider it a reference librarian for the maritime industry"

As part of our ongoing exploration of information sharing tools, we present new and existing applications for information sharing. One tool, MarView, was presented by a MIST sponsor, the Department of Transportation. Piloted in 2006, it is a web portal for collecting, storing, protecting, analyzing, and delivering critical maritime information to commercial, local, state, and federal agencies. It also offers analytic capabilities and permits visualizations of the Marine Transportation System.

Participants were encouraged to try the site out and offer suggestions for improvements.

Recommendations for information design

10. Centralize access to MDA information
11. Provide feedback after MDA information is shared
12. Provide specific information that is needed by the commercial sector (all hazard, navigation related, current and future MDA)
13. Ensure high quality data that supports decision making
14. Utilize best practices for information design for Homeport (see usability.gov)

Trust and cultural understanding

"It's all about the love in Philadelphia."

In all of the ports visited by MIST, private sector participants identified the importance of trust and relationship building. In Delaware Bay, participants noted how their relationships are impacted by how familiar the government players are of the needs and practices of the private sector, how much they participate in the local culture of cooperation, and how well they communicate. First, to help with familiarity, the Delaware Bay private sector has initiated a "Maritime Familiarization Day" and offered vessels for drills. Second, information sharing and cooperation is integral to their culture: "Delaware Bay is a tough and critical culture with a common interest in making things better." Finally, the Delaware Bay consists of four states working together so by necessity they need to communicate broadly: "We go to meetings, meet people, talk to people, and get to know them the 'old fashioned' way."

Recommendations for building trust

15. Expand the Maritime Familiarization Day to government stakeholders
16. Increase private sector participation in drills and exercises
17. Increase private sector outreach efforts

Local models for information sharing

As part of our goal of uncovering local best practices, participants discussed the pros and cons of three local models for information sharing. Participants broke up into three break-out groups and discussed the local AMSC, fusion centers, and two private sector associations.

Local AMSC

The Area Maritime Security Committee (AMSC) for USCG Sector Delaware Bay is a partnership of governmental, labor; commercial and recreational waterway users. The focus is on maritime security and the AMSC participates in information sharing, networking, training, and trust building in the maritime domain. The AMSC is one of the most important arenas for information sharing and has strong and diverse industry participation. In addition, its subcommittees are robust and active. Areas that participants identified for improvement include the need for greater representation of trucking, FSO's and VSO's, and better methods of getting more consistent attendance.

Fusion Centers

Fusion centers attempt to institutionalize information analysis and sharing, primarily in the law enforcement arena. Participants identified four different local fusion centers:

- The Delaware Information and Analysis Center (DIAC)
- The New Jersey Regional Operations Intelligence Center (ROIC)
- The Pennsylvania Criminal Intelligence Center (PaCIC)
- The Maryland Coordination and Analysis Center (MCAC)

The traditional focus of fusion centers is on analyzing law enforcement trends and disseminating analytical reports. The Delaware Bay Region is a model of collaboration in standing up the Delaware Valley Intelligence Center (DVIC), which will bring together the efforts of all four local fusion centers. Participants, in their discussion of fusion centers, identified a need to improve the participation of the maritime community, a desire to standardize processes, a need to improve interagency collaboration, and a lack of consistent funding.

Private sector associations

Participants reviewed two closely related private sector associations—the The Maritime Exchange for the Delaware River and Bay (MEX) and the Mariners Advisory Committee (MAC). Their members are similar and consist of international trade and related business partners throughout Pennsylvania, New Jersey, and Delaware. The MEX focuses on daily port activities and the MAC focuses primarily on safety. The MEX and the MAC both serve an advocacy role for the business community and are a central voice to decision makers in government and industry. The primary area for improvement that participants identified was for wider participation of state government, trucking, and importers/exporters.

Recommendations for local organizations

18. Expand membership of private sector associations
19. Strengthen the maritime focus of fusion centers
20. Include more private sector participation in fusion centers
21. Address issues of information classification levels

Spotlight: a small crew tug

Sailing on the Christina River on a 180 ton tug, moving against the currents, feeling the wind pushing against the boat, and having a 6 deck container ship looming over you is an unforgettable experience. Sitting in the pilot house you can understand why the captain considers himself the eyes and ears of the water: *"Tug and barge operators are on the water 24/7. We're constantly moving around the ports… if we see people in the door of a tanker doing something that's not a normal course of business, that's a security issue and we'll call."* On small crew tugs, however, there are often only two people on board—the deckhand and the Captain. The Captain can often be too busy to answer the slew of questions that the Coast Guard asks when reporting an incident. Dealing with high winds, blinding rain and a 10,000 ton container ship, there is no way that they can spare the mental energy for answering seemingly irrelevant questions about the water temperature or the wind direction. They don't want to talk to Washington, they want to get home: *"They are going to or coming from a job, trying to get to the dock so they can go to sleep."*

Security

The security officer though is just a phone call away. On call 24-7 they are the primary contact point for the tug crew. Often "raised green," they have come up through the ranks. They are familiar with the people and ways of the water. They began in safety and operations and only after 2004 have they assumed the role of security. Their security plans were created in partnership with the American Waterway Operators and are interfaced with Port security plans. In the case of an incident, the crew of a tug is told to call in to the security officer first. Once that happens the security officer works the plan: *"I get the guys that may be in danger and notify them first, then we can go through the other agencies, starting with local Port security, then state security, then the State terrorist tip line, then the Coast Guard, then the National Response Center, etc. The Crew doesn't have to paint the picture for the duty watch stander at the Coast Guard office. I can do that..."*

Resistances

Security though is a touchy subject with certain companies. The new regulations are often seen as costly, unnecessary, and anti-American. The cost of security planning and the impact on daily operations impacts the company's bottom line: *"Security planning is seen as an invasion because we don't see any dollar advantage to it… For instance, we can't just go up to a port anymore and wait for our next job. We have to leave and drive an hour or more to come back."* Several examples were provided that also illustrate how the new security focus conflicts with American ideals of freedom and community:

> *"We had an American flagship, an American crew, American captain come into our auto dock, right here in the good old United States, but because CBP had not received the 48 hour advance notice of arrival, every one of those American citizens were held on that ship and not allowed to come ashore…They were Americans in their homeland and were not allowed off the ship because of a notification. That's absolutely ridiculous. We're prisoners in our own land because of regulations."*
>
> *"(Our boss) has been up and down this river for 40 years. He wants folks to see his company as people and boats. Once a 19 year old boarding officer didn't know him and wasn't going to let him on that ship because he didn't have identification. Now all of a sudden we become the enemy. We're U.S. citizens and we belong here."*

Support

The tug operators we spoke to are social and very involved in maintaining safety and this can benefit security efforts. The operators work with agents, shipping companies, leasers, ports, pilots, and government representatives. They are long time residents of the area and have a lot of pride in their work and their port. The AMSC has been a great forum for them and they value the open communication that they find there. The safety community also plays a strong role in their lives. They have voluntarily complied with inspection guidelines for towing vessels and are working with the Coast Guard, the American Waterway Operators, and the Passenger Vessel Association to help develop plans for security inspections. Even though they feel like government regulations are "shoved down their throat", they understand the need from a safety perspective:

> *"We're the safe operators, we're the ones that don't want our insurance rates increased, we're the ones that want to protect the environment, and we're the companies that want to be safe on the waterway."*

Next steps for the Ports of the Delaware Bay

At the conclusion of the workshops, participants discussed what was needed for them to move forward in strengthening their information sharing capabilities. The participants outlined specific actions related to improving information and communication, building trust, streamlining government processes, and developing incentives for sustaining the effort. Following are the next steps to be taken by the Delaware Bay participants:

Table 1: Action Plan

	ACTION ITEM	TIME FRAME	SUGGESTED FOLLOW UP
Information and Communication	‣ Address Clearances	Q2 2011	**DVIC**: MOU policy to AMSC **USCG**: follow up on AMSC clearances **States**: explore DHS clearances
	‣ Expand maritime and intermodal sharing	Q4 2010	**FBI**: will arrange special interest group for InfraGard **AMSC***: attend Philly InfraGard meeting **AMSC***: will follow up on InfraGard presentation
	‣ Create a feedback System	Q4 2010	**DVIC**: share best practices report
	‣ Increase situational Awareness	Q4 2010	**DVIC**: follow up with CBP; specifically on suspicious crew or cargo, and repatriation of crew information sharing and process **MEX**: bring issue to AMSC for action **MARAD**: engage as a resource for National Strategy for Maritime Security implementation
	‣ Communicate with Trucking	Underway	**AMSC***: Port Business Operations Subcommittee is addressing
Trust and Culture	‣ Identify shared Resources	Completed	**MIST**: will include a shared resource list within the training appendix in final report
	‣ Expand exchange Program	Q1 2011	**FBI and MEX**: gauge interest level, create plan of action based on Maritime Familiarization Day effort **AMSC***: Training and Exercise Subcommittee to consider implementation of such a program
	‣ Decrease episodic AMSC Participation	Q4 2010	**AMSC*:** contact top level regional USCG and CBP by approaching USCG Law Enforcement Liaison Officer to COPT, then COPT to CBP **AMSC*:** Explore best practices of other AMSCs **AMSC*:** Review and update contact list
	‣ Increase coordinated Exercises	Q4 2010	**AMSC***: Planning & Exercise Subcommittee will create a list of what's ahead **MEX**: will share their calendar with others who post calendars online **DVIC**: will make sure all exercises are on all calendars **INDUSTRY**: will work with AMSC to provide industry vessels for drills when possible
Streamlining	‣ Advertise training opportunities	Q4 2010	**MIST**: create a training appendix to include in the MIST report
	‣ Utilize VIPR Teams	Q4 2010	**FEDERAL AIR MARSHAL**: will explore integration with AMSC
	‣ Align federal efforts	Q4 2010	**MARAD**: will connect DVIC with NMIC
Incentives	‣ Support sustainability	Q4 2010	**DVIC**: will support the AMSC in addressing sustainability **AMSC***: Managing Board will decide how to address strategic planning for sustainability
	‣ Create an action Plan	Completed	**MIST**: distribute completed action plan

***All AMSC action items are contingent upon the review and approval of the AMSC Managing Board**

Next steps for MIST

The MIST process is evolutionary and iterative. We value the lessons we learn from each activity and adapt our methods based on what we learn from each local activity. Some of our past learning includes improved processes for participant recruiting, clearer advisory board roles and responsibilities, the increased use of face-to-face interaction, the decreased use of web-based social media, and the inclusion of actionable results. Based on our latest effort, we have identified several areas for improvement.

Next steps for MIST

- Strengthen our local partnerships with the USCG, TSA and CBP
- Schedule events around the availability of key partners
- Increase incentives for participation (testimonials, thank you tokens, food)
- Improve workshop logistics (ensure that wireless is available for usability tests)
- Improve the flow of the workshop (facilitator training, elimination of keynote speaker)
- Utilize federal partnerships more effectively (resources, workshop attendance, funding)

Detailed Findings

The goals of the MIST workshops are to identify key issues in information sharing and to engage the participants in specific problem solving activities. Because information sharing is one form of collaboration, we began the workshop by asking participants to rank the relative importance of several collaboration issues that have surfaced at other ports. As seen in *Figure 2: Collaboration*, private sector participants identified the following issues as most important for collaboration:

- Better information sharing and communication
- Increased trust and cultural awareness
- Streamlined government processes

Government participants also indicated that there were one additional collaboration issues:

- Minimizing jurisdiction wars

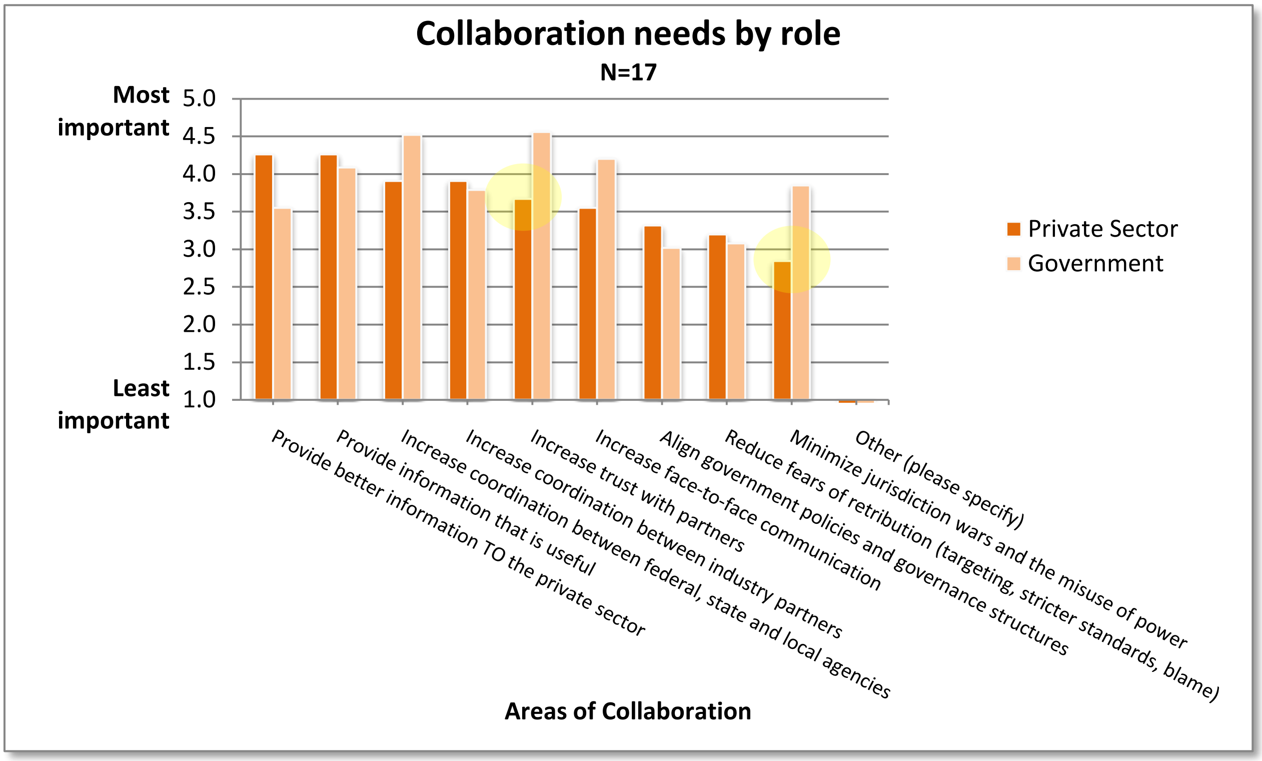


Figure 2: Collaboration

In addition to these issues around collaboration, we had participants engage in discussions around their motivations for information sharing and the specific areas where government could streamline their processes. Based on all of their discussions, we present the detailed findings on the following collaboration issues:

- Information & communication
- Trust & Culture
- Government processes
- Incentives
- Multi-modal issues
- Models for information sharing

Information & communication

“Maybe I’d have done things differently had I known—I’d have been more alert”

When asked if they needed more information sharing around port security, both government and private sector participants indicated that information sharing was important. When asked what specific issues were important, participants highlighted the need for timely information. Our participants also indicated that accuracy/reliability, access to information, the usability of information, reporting procedures, and information overload were all important factors to consider. Verbal responses during the workshop provided more details on how information access and the quality of the tools impact these needs.

Access to information

“We have no information when a threat is suspected until they show up and then the ship can’t move and it’s costing us money.”

Key barriers to information sharing in Delaware Bay are getting access to the information and receiving on-going feedback of the status of alerts or threats. Delaware Bay participants, like their counterparts at other ports, want timely access to information, want information pushed to them, want a central repository for information and requirements, and need to have some access to classified information. Both private sector and government participants recognized that there were gaps in the sharing of information. These gaps include getting the information when it is needed. An example of this is a case where a tanker had been delayed in the bay due to a bomb threat and the terminal security personnel were not notified until it docked. Fusion center personnel noted that often the private sector does not get fusion center products. Finally, participants noted how the CBP and USCG either failed to pass on or delayed passing on specific threat information that would have helped the private sector make informed decisions. Unfortunately, there was no representation from CBP or USCG in the workshop at this time to explain their process and what factors may be involved in delays of sharing information.

Another access issue that surfaced was the lack of feedback once information was shared. Private sector participants noted how often, when they do report incidents, they never hear back from government agencies about the final resolution: “We had a barge captain call in about a guy taking pictures but there is no feedback—we can’t go back to the Captain and say ‘you did a good job and this is what happened.” They stressed the importance of staying in communication with the people in the field: “let the guy know in the port that we are doing a good job.” Government participants recognized that this is an important aspect and were able to sympathize with the private sector: “There is nothing more satisfying than calling a homicide victim with confirmation that the case is closed—we need to respond to those that report otherwise they will stop reporting.”

Participants identified several areas where specific improvements could be made in sharing threat information:

Share information systematically

- Push information out to industry
- Provide information in a timely manner
- Improve clearance processes
- Improve the processes for stripping classified information
- Address issues of sharing PCII information
- Set up lines of communication before an event

Communicate more effectively

- Provide time-sensitive information directly by phone
- Provide feedback on the outcomes of threat reports
- Encourage the relevant agencies to share information ahead of time
- Designate a central contact person
- Use multiple forms of contact (physical, email, phone)
- Support personal communication

Utilize existing systems

- Utilize the NMIC, DVIC, ROIC, Alert Philadelphia, Ready PA, or other existing communication frameworks to disseminate information
- Model New Jersey's monthly summary of threats region-wide

Many of the government participants recognized the importance of sharing information but noted the many obstacles in their way:

- The risk of distributing incorrect information
- Legal ramifications
- Lack of existing mechanisms for disseminating to private sector
- Amount of time needed to strip classified
- Lack of trust that information will be kept "close hold"

Quality of information and tools

"We get Intel information that we have no idea what to do with…give us actionable information"

Participants provided input on the quality of information through an informal poll, during group discussions and by doing a scenario using Homeport. Issues that surfaced included making information relevant, consistent, and easy to use. The relevancy of information was of primary importance to the participants. Private sector participants wanted information that is useful, specific, actionable, and includes follow-ups (see *Figure 3: Information Types*)[18] Useful information relates to anything that affects navigation. They want to know "What is going on now and what is going to happen next." The private sector also wants information that is actionable: "I want information I can take and do something with rather than broad educational information." Finally, as noted above, the private sector needs to be kept in the loop and notified when an issue is resolved.

[18] Interestingly, the government participants initially ranked specific threats and impacts on the movement of goods much lower than the private sector.

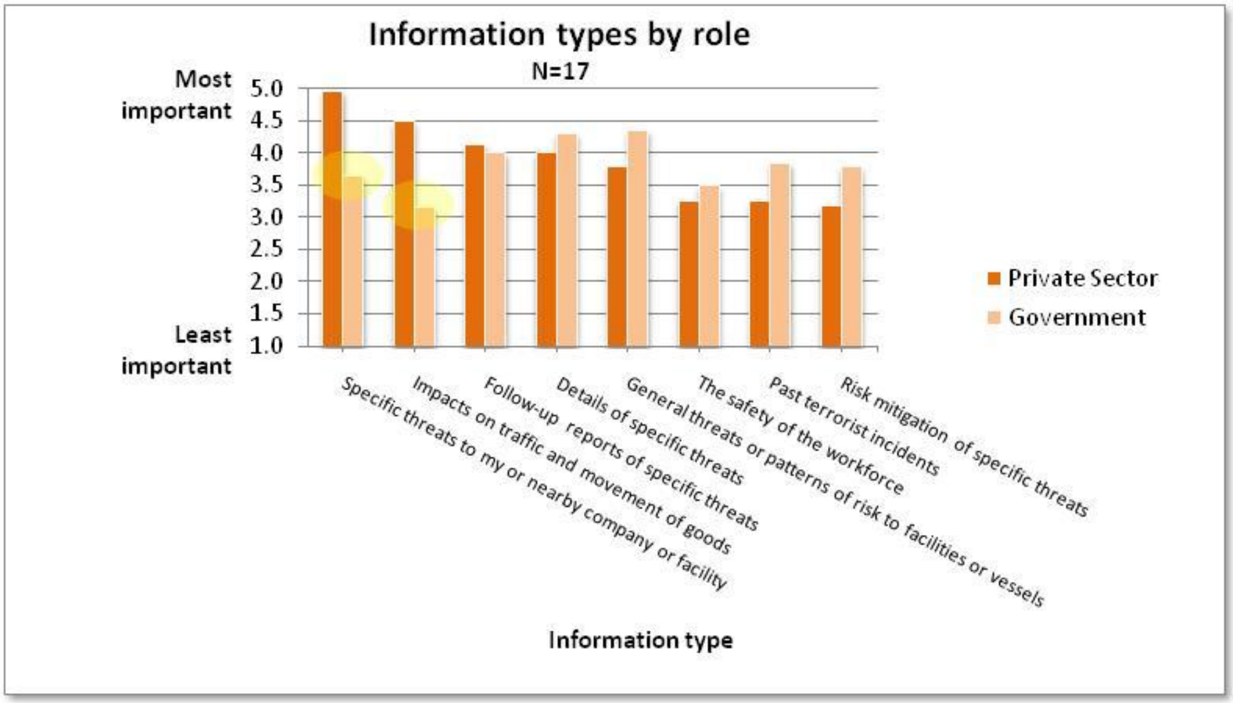


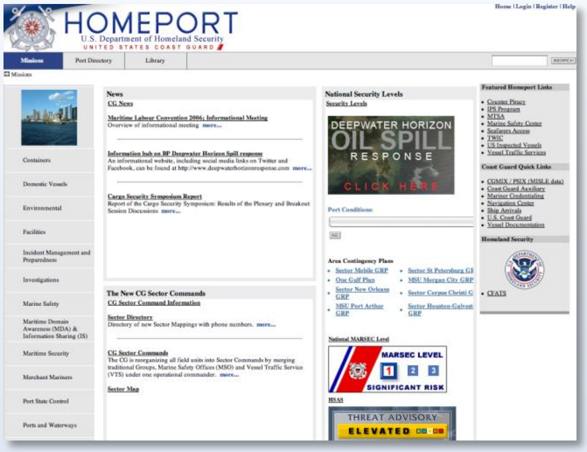
Figure 3: Information Types

Consistency is also a key element in information quality. Participants want to see accurate and consistent information otherwise they start to mistrust the data. During the Homeport scenario, participants could not locate ships that they knew were in port. This discrepancy made them mistrust the accuracy of the data and reluctant to use the site. Also, each local Homeport site contains different types of information and this inconsistency leads to false expectations of what can be found at the site.

Case Study: Homeport

During the workshop, we had two participants use the Homeport site while doing two scenarios. Scenario 1 had a participant go to the Home page and talk about what the site offers. Scenario 2 had the other participant use the site to locate specific threat information. Overall, participants had difficulty using the site and found it only somewhat desirable and useful.

Desirability
Users initially like the idea of accessing information specific to their port, but technical difficulties with the site led quickly to frustration. The site was being accessed through the local USCG facility and the load times were very slow. In addition, the interface kept locking out the users when they tried to use the "Back" function. Since both of these barriers are likely to occur in the field, they may be a significant source of frustration and result in a reluctance to use the site. In addition, the users noted that there was too much on the Home page.



News
CG News

Maritime Labour Convention 2006; Informational Meeting
Overview of informational meeting more...

Information hub on BP Deepwater Horizon Spill response
An informational website, including social media links on Twitter and Facebook, can be found at http://www.deepwaterhorizonresponse.com more...

Cargo Security Symposium Report
Report of the Cargo Security Symposium: Results of the Plenary and Breakout Session Discussions more...

The New CG Sector Commands
CG Sector Command Information

Sector Directory
Directory of new Sector Mappings with phone numbers. more...

CG Sector Commands
The CG is reorganizing all field units into Sector Commands by merging traditional Groups, Marine Safety Offices (MSO) and Vessel Traffic Service (VTS) under one operational commander. more...

Sector Map

National Security Levels
Security Levels

Port Conditions:

Area Contingency Plans
- Sector Mobile GRP
- One Gulf Plan
- Sector New Orleans GRP
- MSU Port Arthur GRP
- Sector St Petersburg GF
- MSU Morgan City GRP
- Sector Corpus Christi G
- Sector Houston-Galvest GRP

National MARSEC Level

HSAS

Featured Homeport Links
- Counter Piracy
- IPS Program
- MTSA
- Marine Safety Center
- Seafarers Access
- TWIC
- US Inspected Vessels
- Vessel Traffic Services

Coast Guard Quick Links
- CGMIX / PSIX (MISLE data)
- Coast Guard Auxiliary
- Mariner Credentialing
- Navigation Center
- Ship Arrivals
- U.S. Coast Guard
- Vessel Documentation

Homeland Security
- CFATS

Usefulness
Users found Homeport minimally useful. Useful features included:

- Alerts and notifications
- Connecting all sectors together

Ease of Use
Users found Homeport somewhat difficult to use. Users struggled with the navigation, terminology, search, and lack of content. These difficulties impact how users view the site. Specifically, users had difficulty with the site leading to several negative reactions:

Seeing the site as not credible

- Not being able to locate ships they know are in port
- Outdated information on ports

Seeing the site as not useful

- Inability to view two pages at once
- Seeing pages with no information on them
- Difficulty locating threat information (located on the right, not the left menu)
- Inconsistencies in how different ports use the site

Getting frustrated

- Inability to use the "Back" button (caused the site to lock up) leading to frustration
- Mistakenly navigating from the local site to the national system, resulting in confusion
- Slow load times

Figure 4: Case Study Homeport

Trust and cultural understanding

“It’s all about the love in Philadelphia.”

In all of the ports visited by MIST, private sector participants identified the importance of trust and relationship building. In Delaware Bay, participants described how their relationships are impacted by how familiar the government players are of the needs and practices of the private sector, how much they participate in the local culture of cooperation, and how well they communicate.

Familiarization

Many private sector security personnel have had a long history of being involved in maritime affairs. Facility Security Officers often have lengthy experience in maritime operations and Port officials have spent a good part of their careers working in the maritime environment. The private sector expects their government partners to have a core understanding of their environment and their issues. The Delaware Bay area has made a concerted effort to familiarize people with their environment. They have hosted a “Maritime Familiarization Day” to introduce people to the ports of Delaware Bay and have offered up vessels for law enforcement drills. These outreach efforts have been viewed positively by the government officials in attendance: “I wouldn’t have noticed that I couldn’t get through ship doors with my assault gear without being on the vessel.” The outreach has also helped them understand the environment and has impacted planning activities: “Getting out in to the field can dispel many misconceptions that crop up in scenario planning.”

Community focused culture

The participants noted how the Delaware Bay area has a unique culture of the “little guy doing the right thing”. They have a strong community bond and are proud of it: At the same time they are a very direct culture and the “people are not afraid to tell you if it’s junk.” Because “Delaware Bay is a tough and critical culture with a common interest in making things better”, information sharing is a core cultural activity.

Communication

Maritime security in the Delaware Bay region is a four state endeavor and by necessity the maritime community needs to have well functioning communications. For the participants this means both face-to-face and structured communication. When asked specifically how the participants increase trust the answer was in personal communication: “Go to meetings, meet people, talk to people, get to know them.” The “old-fashioned” way of discussing issues is still important. Dinners, hallway conversations, and coffee meetings are key ways to communicate issues when they arise: “I expect people I know to call if there is something I need to take action on.”

More formal methods, such as the AMSC, the Mariners Advisory Committee (MAC), Alert Philadelphia, and the Maritime Exchange are important venues for information sharing but are seen as underutilized.

Streamlined government processes

“So many different government agencies that we have to answer to, and when you answer to one of them they send you to another one.”

We began our discussion of government processes by having the participants review and comment on previous challenges in working with government agencies. These challenges are shown in *Figure 5: Streamlining targets*. When private sector participants were asked to rank issues raised in other MIST workshops, the private sector identified the following needs as critical to successful information sharing:

- Improve interagency coordination of information and communications
- Improve the coordination of policies and procedures
- Improve the coordination of roles and responsibilities
- Improve intermodal collaboration

The government participants mostly shared these concerns but placed less importance on the need to simplify government processes and regulations. They also recognized the importance of improving information sharing internally. Following is a discussion of the key areas ripe for streamlining.

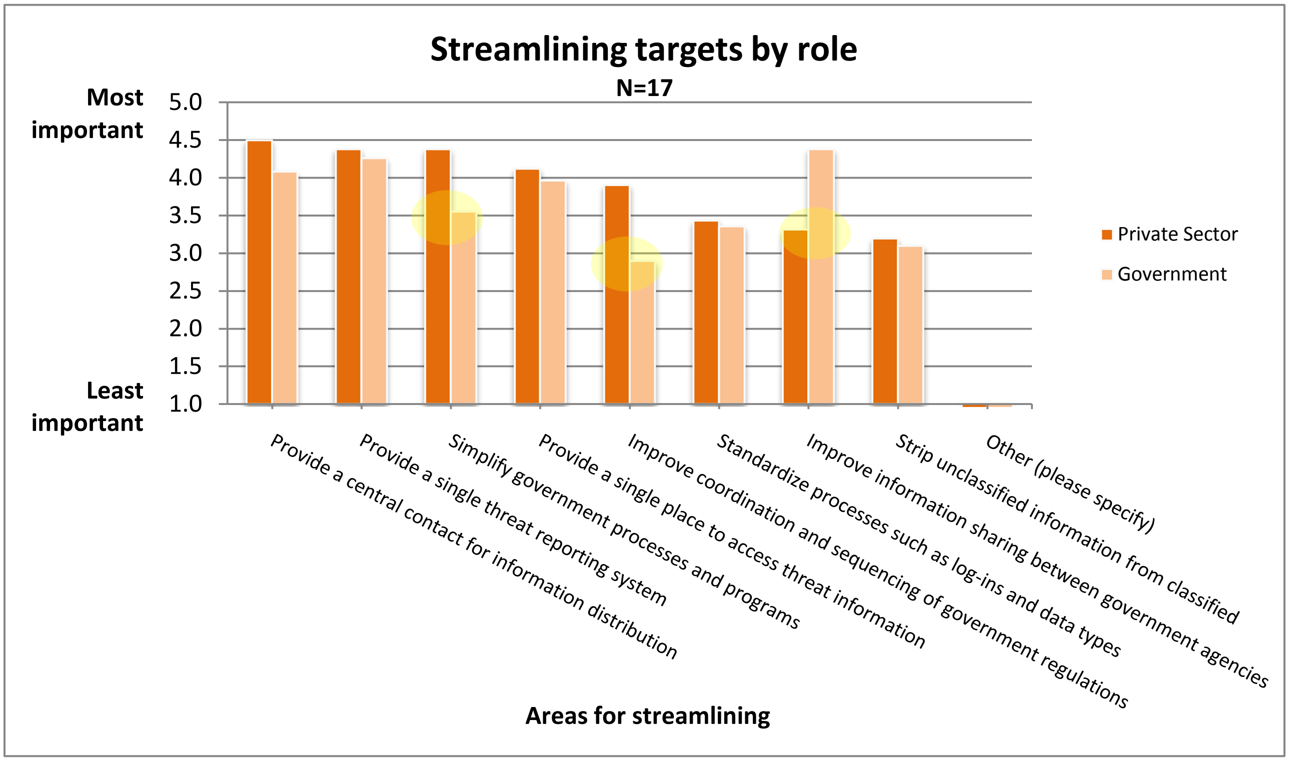


Figure 5: Streamlining targets

Interagency coordination of communication and information

Three of the top four items targeted for improvement in Delaware Bay had to do with coordinating the means of communication. Participants here, like their counterparts at other ports, want a central contact person for getting information, a single place to access threat information, and a single threat reporting system. The private sector has a number of places that they can get information but the information they get can be conflicting. There is a need to standardize and institutionalize the information sharing process, especially when you consider personnel turnover. The DVIC is attempting to do this through the use of needs analysis and close interactions with area security personnel. The need for a coordinated response was recognized by the government participants who shared some of the private sector's frustrations with coordinating government agencies.

The general sense of private sector participants was that they were often being left out of the loop: "It's unfortunate that CBP isn't in the room and we don't have anyone left from the USCG—we have no information when a threat is suspected…" This issue of interagency collaboration was recognized by participants as an important factor in any multi-agency activity. Representatives from the DVIC shared that they planned to address this challenge as part of the standing up of the fusion center.

Participants also noted several agencies where the coordination was working well:

- FBI (WMD coordinator and industry outreach)
- U.S. Federal Marshal's VIPR teams
- DoD coordination of fuel movements
- Intelligence products from the DIAC

Interagency coordination of policies and processes

High on the private sector participant's list of preferred improvements is the need for government to coordinate their processes, programs, and regulations. In general, participants felt that there were too many government agencies to answer to and that many of the regulations conflicted with each other. Many of the government processes also reflect "unrealistic expectations" of what can be done in the maritime environment. Three examples that participants provided illustrate the impact of these regulations:

> *Crew pick up*
> The process for handling crew pick up at ports is inconsistent and expensive. The cost of escorting and transporting crew on and off facilities can range anywhere from $800 to $2000 a trip.
>
> *Crew repatriation*
> Repatriation (arranging for crew members to return to their native countries) is a common occurrence in Delaware Bay and the process is currently very cumbersome. Often, getting armed guards for repatriating crew members can cause delays and increased costs due to inadequate notifications.
>
> *TWIC*
> The transportation worker identification card (TWIC) process is a long standing example of a government regulation that was extremely challenged in implementation. Because of this, TWIC has had a strong impact on the private sector.

Interagency coordination of roles and responsibilities

In discussions surrounding the streamlining of government processes, the Delaware Bay participants noted that overall there is good coordination between the four state governments. The Area Safety Committee, Mariner's Advisory Committee, DVIC, and Alert Philadelphia, were all viewed as good examples of coordinated activities. The general belief was that locally the coordination was working well but that it might help to visit other AMSC's to see best practices. Government participants noted that their world was becoming more complex due to new legislation and new technologies: "It's a patchwork."

Intermodal coordination

For the first time the workshop specifically addressed issues with the coordination of private sector intermodal partners. The participants described the complexity of the interaction: "it's a ripple effect from maritime, to rail, to mass transit, to trucking" that impacts the movement of goods. Each mode's operations and risks are dependent on the other. In operations, trucking was viewed as a particularly difficult thing to coordinate because each company has its own procedures. Terminal operators want to know when the truck is coming and who the operator is. This information is often not received. In addition, not all truckers have TWIC cards and this requires terminal operators to hire an escort resulting in delays and increased costs. Getting TWIC cards for rail operators was particularly difficult.

Often, when dealing with intermodal partners the nature of risk is also not evident. For instance, in the movement of oil, the pipelines extend all over—under the ground, above the ground, and near transportation. The transport of oil was the primary concern but not a large one—maintaining supply was not seen as a risk because of the redundancies in the system and a history of operating safely. However, participants did have some concern for environmental impacts in the case of a spill. However, a Federal government stakeholder saw the potential vulnerabilities and noted that they were currently examining these vulnerabilities.

Participants noted several processes that worked well including the following:

- GPS tracking of trucks
- Hazmat tracking
- DOT-PHMSA pipeline sensors

Incentives and private sector values

Incentives, both material and social, are important motivational factors in the adoption of new processes, policies, and technologies. Early on, the MIST and Global Maritime Information Sharing Symposium (GMISS) programs sought to better understand what might motivate the private sector to share information. As in our previous two workshops, we encouraged participants to look at the benefits of information sharing from a wide perspective. To help expand the concept of benefits, we presented participants with a 360 degree value model for evaluating incentives (see *Figure 6: Value Segments and System Impacts.*) This value model segments incentives into five areas—financial, operational, social, ideological, and strategic. These value segments may impact the system across five organizational zones—individual, group, organization-wide, enterprise-wide, and global. Using this model, we encouraged participants to look more closely at their motivations.

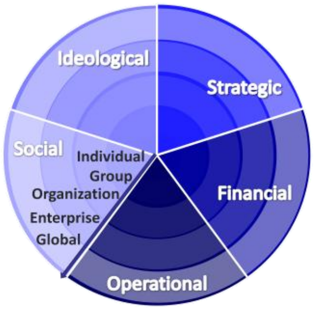


Figure 6: Value Segments and System Impacts

This port had a well balanced set of desired incentives, emphasizing financial, operational, and social incentives (see *Figure 7: Incentives by Role.)* Of particular note is the fact that private sector participants viewed quicker business resumption, fewer costs incurred, and increased port use differently than government participants. This may indicate a mismatch of goals between government and private sector participants.

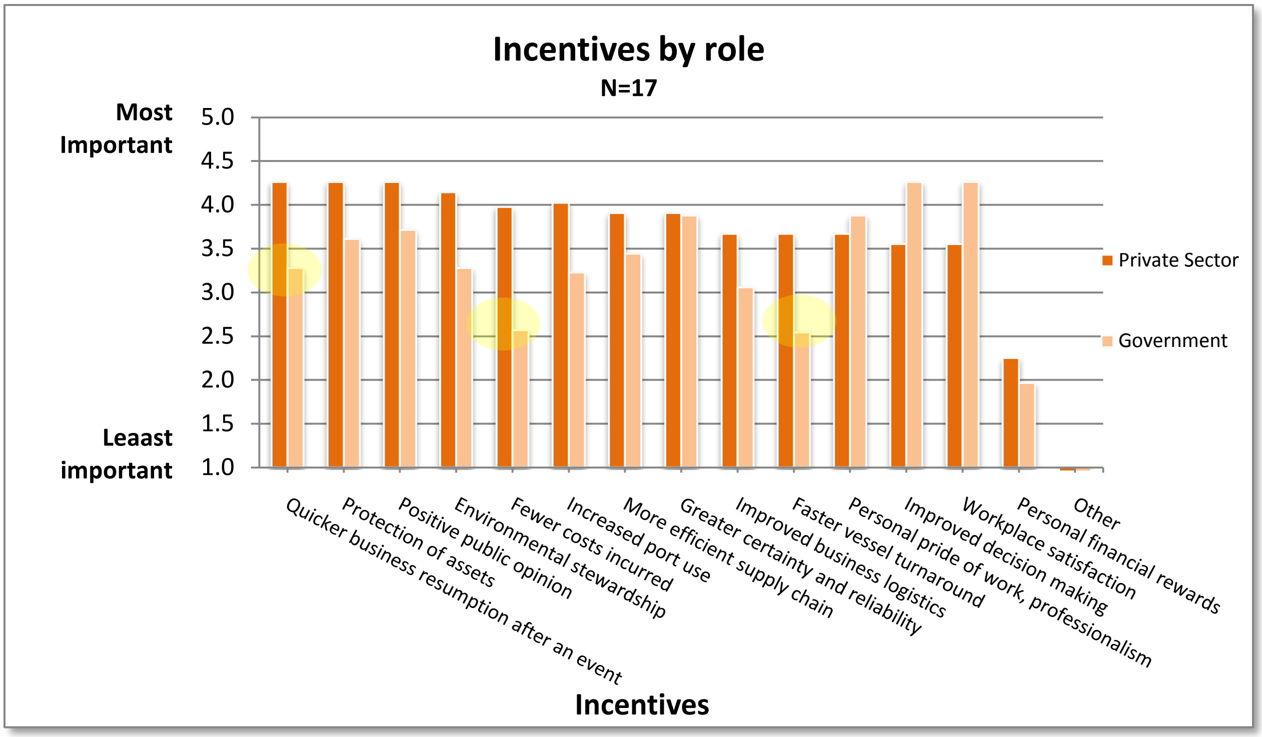


Figure 7: Incentives by Role

Operational benefits

"If you know what to expect, you may make better decisions and plans"

Operational benefits are material rewards that increase the efficiency and effectiveness of the organization. Delaware Bay participants indicated that operational benefits were an important motivator for participating in port security operations. Participants discussed how efficiency, predictability, and safety and security were important to their business operations. Efficiency factors included more efficient use of the marine transportation system to move goods and people, and increased productivity. Improved decision-making leads to more predictability allowing companies to "better allocate assets and better planning" for things such as security staffing and sailor transportation. And, safety is a core responsibility for many security professionals so anything that makes the workplace safer and reduces risk is important. Significantly, participants also recognized how if "information is shared with the right people at the right time" their jobs can be done more effectively.

Financial benefits

"We're in the business of making money"

Financial benefits are material benefits that are related to monetary rewards. When presented with the list of financial benefits from other workshops, the Delaware Bay participants generally agreed that financial benefits were a very important incentive for information sharing. Attracting and retaining business, maintaining a resilient community, and ensuring business continuity were important factors for industry. Government agency personnel valued an effective marine transportation system and law enforcement saw a reduction in smuggling and crime incidents as key return on investment (ROI) factors.

The participants also noted how both operational efficiencies and environmental concerns were related to financial benefits. Operational improvements mean less time, and less time means more money. In the case of environmental actions, participants noted that faster throughput results in lower fuel costs which not only improves the environment but also means less fuel burned in the port. These are two examples provided by industry that illustrate the importance of tying incentives to the underlying financial gain for the private sector.

Strategic benefits

"Stability helps reduce risk making us a more attractive facility, organization, or region"

Strategic benefits are plans or patterns that further the success of the stakeholder. In Delaware Bay, participants shared several strategic motivations with our other ports:

- Greater certainty and reliability
- Improved customer service
- Positive public opinion

Greater certainty comes from knowing what to expect. Any reduced variability in their business can lead to reduced schedule and performance risk and limit their liability. Another benefit of sharing information is the increased confidence of their customers and improvements in the reputation of the port or facility. These increases impact the bottom line and are a key factor in deciding to participate in information sharing programs. In addition, participants noted that improved knowledge management was an incentive: "Many hands make light work… sharing best practices across the region can result in increased awareness for all."

Social benefits

"It's important to feel that you can have a say: that you are listened to."

Social benefits are those benefits that take into account the interests, intentions, or needs of people. In Delaware Bay, participants saw value in things that improve workplace satisfaction, build trust, improve teamwork, offered opportunities for recognition, and/or improved their safety and security. Workplace satisfaction issues ranged from wanting to "surface problems that may not be visible to management" to the simple satisfaction of doing a job well. Increased morale and reduced frustration are also key elements of workplace satisfaction.

Trust and reduced fears were important goals for Delaware Bay and teamwork was one way that surfaced to build trust. Participants found that combined efforts led to more trust: "To feel a part of an organization, to have a say…to be part of a team" is important in building personal connections and trust. This team spirit was seen as a core element in cooperation and information sharing.

Ideological benefits

"We're the greatest unknown port we know"

Ideological benefits relate to the ethical values of the stakeholder and include political, cultural, as well as moral beliefs. For Delaware Bay, the above discussed emphasis on the social benefits of information sharing is informed by the areas strong sense of pride. Our participants noted how they are "the little guy doing the right thing" and an area where "everybody works to make things better." They see themselves as "the little port to the south" (of New York), and although not very well known, of key importance in the movement of goods. They tend to see themselves as team players who want to make things better rather than pointing out what doesn't work. They seem to place a lot of importance on getting things done cooperatively, taking personal responsibility, and taking pride in their port. This perspective is similar to that found in the Port of Honolulu, but with an added "underdog' component.

In addition, the participants noted that environmental issues were important to them. Being an environmental steward is not only "the right thing to do" it is seen as good for customer perceptions and is directly tied to financial benefits.

Measures of effectiveness

Measures of effectiveness are quantifiable measures of success. They should be realistic, measurable, and relevant. Measures of effectiveness allow us to assess the impact of specific initiatives and see if our efforts are leading to desired results. In each port, participants have identified effect measures that are important. Although not probed directly, participants from the Delaware Bay region added an additional item (layers of access to information) to our list of measures of effectiveness for information sharing. This brings the total to 14 items covering four areas:

- Ease of access to information
- Operational efficiency
- Response capability
- Preparedness capability

Participants from the Port of Delaware Bay offered one new measure of success for information sharing: The number of layers of bureaucracy to access information. We now have 14 metrics to consider when looking at progress in information sharing:

Ease of access to information

- The number of layers to access information
- The number of users on distribution lists for alerts
- Time to access contact person

Operational efficiency

- Less time at anchor
- Fewer delays
- Fewer ships at anchor
- Reduced violations (due to better information)
- Sharp rate of decline in violations (when new policies are implemented)
- Decline in ground user complaints

Response capability

- The number of responses to calls for information
- Time duration between alerts and response
- Total response time
- More successful drills

Preparedness capability

- More robust preparedness levels

Models for information sharing

As part of our goal of uncovering local best practices, participants discussed the pros and cons of three local models for information sharing. Participants broke up into three break-out groups and discussed their local AMSC, fusion centers, and two private sector organizations.

AMSC

"The AMSC has a common goal of maritime domain awareness."

The Area Maritime Security Committee (AMSC) for USCG Sector Delaware Bay is a partnership of Federal, State and Local law enforcement and intelligence organizations; governmental, regulatory, public safety and emergency management agencies; organized labor; commercial and recreational waterway users; and, public and private sector stakeholders who are committed to improving the security of the maritime transportation system. During the workshop the AMSC break out group identified the common focus areas, key activities, and missing elements.

Background and focus
The participants described the AMSC as operating at three levels: general meetings for information dissemination and training, a managing board that operates at the strategic level, and subcommittees that function as working groups. The AMSC includes a cross representation of groups including government security personnel and private sector representatives from land, water, and intermodal operations. The focus of the AMSC is on information sharing, networking, and trust building in the maritime domain.

Activities
According to the participants, the AMSC gets involved in information dissemination, training, and coordination of maritime security issues. The managing board serves a strategic function, providing direction, interfacing with external stakeholders, endorsing subcommittee findings and helping to draft grant applications. The subcommittees have specific areas of expertise and address policy and training issues.

Missing elements
The participants identified several missing elements in the AMSC:

- Need for improved representation of trucking, FSOs and VSOs
- Difficulty getting consistent attendance
- Need for innovative outreach efforts, e.g. social networking
- Need for a member directory

Fusion Centers

"Fusion centers deliver Intel products"

Background and focus
Fusion centers attempt to institutionalize information analysis and sharing. In Delaware Bay there are currently four state centers:

- **DIAC**
  The Delaware Information and Analysis Center is an "All Crimes, All Hazards" approach to Homeland Security at the state level. The DIAC provides real time information and intelligence to the Law Enforcement sector.
- **ROIC**
  The New Jersey Regional Operations Intelligence Center is an "all-crimes, all-threats, all-hazards" fusion center that supports law enforcement and homeland security agencies across New Jersey.

- **PaCIC**
  The Pennsylvania Criminal Intelligence Center provides law enforcement agencies throughout the Commonwealth with one central point of contact for intelligence information, investigative data, and public source information.
- **MCAC**
  The Maryland Coordination and Analysis Center is an umbrella organization of local, state and federal agencies, as well as representatives from the private sector, that coordinates activities, develops policy, and implements strategic plans to combat terrorism in the State of Maryland.

These fusion centers share a common goal to increase Intel capacity and a national effort is underway to consolidate these efforts. DHS is attempting to join all 72 fusion centers nationally and the Nationwide Suspicious Activity Reporting (SAR) strategy is to develop, evaluate, and implement common processes and policies for gathering, documenting, processing, analyzing, and sharing information about terrorism-related suspicious activities. Fusion centers are primarily focused on law enforcement and many do not have maritime connectivity. A new fusion center, the Delaware Valley Intelligence Center (DVIC), is currently in the process of being stood up and will be fully active in August of 2011.

Activities
Participants identified a number of key activities of fusion centers. First, the primary focus of these organizations is the analysis of information with the primary product being analytical products. The fusion centers focus on gathering and synthesizing law enforcement tips, threat assessments, global trends, and regulatory impacts. The centers goal is to share information with the ATF, HIDTA, TSA, FBI, DHS, JTTF, FIST-FIG. Information sharing with the private sector has historically been weak. They currently share information through local task forces, face-to-face meetings, and participation in exercises. Often they share information through the USCG.

Missing elements
Participants identified several areas that impacted information sharing:

- Weak focus on maritime issues
- Poor integration of water-land-air
- Lack of consistent funding
- Lack of standardized classification procedures
- Lack of regulations allowing them to share information (e.g. DoD, FBI clearances)
- Interagency coordination difficulties (e.g. NMIC, NMCO, FFA)
- Over dependency on specific people (staff turnover breaks communication)

Maritime Exchange and the Mariners Advisory Committee

"We've been around since 1875, facilitating commerce"

Background and focus
The Maritime Exchange for the Delaware River and Bay (MEX) is a not-for-profit trade association, promoting commerce on the Delaware River and Bay. Their members consist of international trade and related business partners throughout Pennsylvania, New Jersey, and Delaware. Their focus is on port operations and multimodal situation awareness as it affects the movement of goods and people. Although oriented to the private sector, it engages with the entire port community. The Exchange also works closely with the Mariners Advisory Committee (MAC) and shares many of the same stakeholders. The MAC was established in 1964 to focus on issues related to navigational safety. Both organizations share a focus on port operations and the facilitation of commerce.

Activities

The MEX and the MAC both serve an advocacy role for the business community and are a central voice to decision makers. They are not limited to specific communities (e.g. law enforcement, security) but engage the total port community in relationship building. They provide policy guidance to industry and facilitate conversations between industry and decision-makers. They work with mariners, ship service providers (agents, line handlers, etc.), private sector shippers, and the government.

The MEX interacts most with the CBP, USCG, TSA, USDA, FDA, MARAD, and the EPA. MEX is a fiduciary agent and assists with port security grants, advanced notice of arrivals, cargo manifests and training. They distribute daily vessel schedules, safety bulletins, security alerts, 24 hr. AIS, and summaries of port statistics.

The MAC is primarily a safety organization and interacts mostly with Harbor Safety committees, the American Waterways Operators, NOAA, the USCG, and the Army Corps of Engineers. The MAC handle issues surrounding dredging, and other navigation advisories.

Missing elements

Participants identified several areas where MEX and MAC can be improved:

- Need more members from state government, trucking, and importers/exporters
- Need to continue outreach efforts for orienting government regulators and new industry members to the port domain

Next Steps

At the conclusion of the workshop, the participants identified action items in information sharing, trust building, streamlining government processes, and providing incentives for moving forward.

Information & communication

Clearances: create intelligence products that are more widely releasable

InfraGard: strengthen the maritime and intermodal applications

- Create special interest groups
- Schedule InfraGard presentation to AMSC – will target the November AMSC meeting, but to be completed by the end of the year

Feedback System: need consistent two way information sharing

- Build feedback plan into DVIC, will reconnect with stakeholders to design and institutionalize a feedback mechanism that will be functional, sustainable, and meet everyone's needs.
- Present the need to the AMSC and let the Managing Board assign it as they see fit.

Situational Awareness: get information to industry from law enforcement, specifically CBP

- Address suspicious crew or cargo
- Address repatriation of crew

Communication with Trucking: improve channels between terminals and trucking for access control

Shared Resources: create a catalog of regional resources available to benefit all stakeholders

- Start with an AMSC membership directory

Building trust & understanding culture

Exchange Program: expand shipper/law enforcement exchange to increase understanding of different perspectives

- Co-design the exchange program (Federal level FBI interested in an industry perspective orientation, and will work with MEX to design an appropriate experience.)
- Include new maritime analysts
- Ensure a cross-pollination of perspective orientations (Industry should also get a sense of law enforcement perspective)

Episodic AMSC Participation: address consistency of participation in AMSC

- Consider replicating the northern effort (New York City)
- Involve CBP

Coordinated Exercises: re-establish coordinated exercise program

- Base on information sharing focus/model, intelligence
- Coordinate with others who conduct exercises/drills
- Include PS and meet multiple exercise requirements
- Get drills, exercises, and trainings in the DHS national exercise (NEX), HOMEPORT, and AMSC calendars. Already on MEX calendar.

Streamlining government processes

Training: share training efforts

- Create a training catalog for resources available or of benefit to regional stakeholders

VIPR Team: explore integration with AMSC

Federal Alignment: connect the Delaware Bay operational area with NMIC and other federal level efforts

- Create a bridge with MARAD and MEX re: National Maritime Security Policy and National Maritime Security Strategy guidance, then contact with CBP

Incentives

Sustainability: address funding, resources, personnel, participation

- Pursue federal dollars. There is a lot of good stuff going on here in the port – there is a need for Federal dollars to keep coming in here to keep it going
- Assign someone responsibility to search for funding sources
- Address issues of maintaining efforts when champions change jobs/sectors

Action Plan: summarize task list and distribute to all participants in the interim before report is released

Once we had identified the key follow up actions, we then established time frames for action, and suggested which agencies would lead the effort. The following chart lays out the results of this planning effort.

Lessons learned about the process

The MIST process is evolutionary and iterative. We value the lessons we learn and adapt our methods based on what we learn from each local activity. Some of our past learning includes the importance of leveraging the AMSC meetings to socialize the MIST process, formatting flip chart sheets prior to the workshop to capture specific feedback, and including two researchers for each field study event to improve reliability. Based on our latest effort, we have continued to identify areas for improvement.

Outreach

The MIST Delaware Bay Steering Committee was convened in a much more rapid pace than previous steering committees, due to a change in the initial location from the New York/New Jersey Port Region. The New York/ New Jersey Port Authority requested at the end of July that MIST hold off until the beginning of the 2011 calendar year due to multiple projects and exercises underway. We were able to connect with the Delaware Bay Port Region in early August and scheduled a presentation to the AMSC on August 20th and to the steering committee on August 19th. This was followed by the field study the following week and the workshop at the end of September.

The success of this steering committee and MIST process as a whole could be directly attributed to strong personal relationships and a mature AMSC structure. Ms. Lisa Himber from the Maritime Exchange of Delaware Bay had participated in a brief of MIST more than a year prior at a Maritime Information Services of North America (MISNA) meeting. Her understanding of the potential value of MIST and the need for strong local participation in the process was a key driver. She was a champion in convening the steering committee as well as in facilitating opportunities for field study participants.

Past steering committees have had the luxury of convening two or more times prior to the work shop and field study, while this steering committee met only once. The first meeting and only steering committee meeting was held on August 19, 2010. There was representation from the shipping terminal industry, the Maritime Exchange and local law enforcement. While the meeting was hosted at the USCG Sector Delaware Bay conference room, the USCG was not represented due to other work load demands. After the initial meeting, the committee was actively engaged in logistics and recruitment. The MIST program manager reviewed many presentations and documentation from the Delaware Bay region prior to meeting with the steering committee and was able to ask targeted questions of efforts underway. This preparation was important to orientate the MIST team to the Delaware Bay as well as to convey the interest and integrity of the team.

The fast pace of planning and recruitment created a challenge for communication and much of the conversation and results of steering committee activity was not well shared with the entire research team or future participants.

Recommendation

- Share the notes and outcomes of the steering committee with the entire research team
- Provide read ahead materials and a detailed agenda to participants

The headquarters divisions of DOT-MARAD, USCG, NMCO and GMAII were kept aware of MIST Delaware Bay implementation, but were less involved in the overall planning. DOT-MARAD, FBI, Federal Marshals and the Information Sharing Environment (ISE) provided strong representation at the workshop which was very informative to all participants. While the intent of MIST is to convey the voice of private industry, that bridge is incomplete without Federal participation.

Federal MDA information sharing stakeholder's participation in the MIST process is critical to actually bridge the communities and facilitate a better understanding of information sharing.

Recommendation

- Ensure active participation of key stakeholders, especially the USCG and CBP

For MIST Delaware Bay, the greatest barriers to participation were a previously scheduled exercise and an unexpected labor action that affected several terminals. These events where compounded by the need for MIST to be held before the end of the fiscal year to utilize funding sources, which minimized our flexibility in scheduling the workshop.

Recommendation

- Analyze recruitment patterns to identify strengths and weaknesses

Logistics

MIST Delaware Bay was held at the USCG Sector Delaware Bay conference room in Philadelphia. This location was familiar to many participants as this is where the AMSC and other meetings are routinely held. The physical layout was conducive for successful small and large group activities. The technology capability of the room was impressive. There were several viewing screens and the support provided by Bob Ward of the USCG was very helpful. The only technology issue was the instability of the wireless internet, which affected the technology demonstration and usability test of Homeport.

Recommendation

- Confirm the internet capability prior to the workshop to ensure that the small group usability test will go smoothly

The hospitality, parking and supplies provided by the USCG were ideal and appreciated. The USCG sector provided coffee and the research team program manager donated pastries for participants both days of MIST. Food has been a challenge for MIST. The team is well aware when food is provided; participants appear to feel more comfortable. We have regularly observed participants gathered around the coffee or pastry table furthering conversations from the workshop. Unfortunately, restrictions on Federal funding prohibit serving food.

Recommendation

- Explore a means to provide food beyond the MIST team and steering committee contributions

On the day of the workshop, the team was very prepared with name tents and folders. However, there were a few participants who had not RSVPd or were coming in place of others and it would have been ideal to have a sign in sheet listing to add new names and information. It would have also been good to have a check list for the participant folders as it was noted on the second day that we were missing the evaluation form. This was remedied by sending out an e-mail to have people complete the evaluation on-line. This proved to be not as effective as having a paper in session evaluation as we received only 12 evaluations after an initial request and one reminder e-mail.

Recommendation

- Provide a sign in sheet that allows new people to sign in
- Provide a checklist of needed materials
- Include evaluation forms in the packets

AMSC Meeting Presentations

As with MIST Honolulu, the program manager had an opportunity to present at the regional AMSC meeting. This was a really great opportunity that was made possible by the AMSC and the USCG

Sector Delaware Bay. The meeting targeted potential MIST stakeholders and resulted in greater understanding of the process and improved recruiting of participants to the workshop.

The Delaware Valley Regional Planning Commission (DVRPC) also presented at this particular AMSC providing a point of contact that may have otherwise not occurred. The relationship between the overall transportation perspective of the DVRPC and MIST was valuable. Their recently completed report takes an intermodal look at security.[19] In their report they outline ideas to move forward that include more collaboration: "participating in efforts by other organizations and contributing a regional planning view; and reaching out to partners to identify additional ways to help fill gaps and coordinate productively to improve transportation security planning."[20] The MIST team program manager met with DVRPC to better understand their efforts and look for ways to leverage their work in the MIST process. As a result, DVRPC did send representation to the MIST workshop.

Recommendation

- Ensure that Metropolitan Planning Organizations are included in future MIST processes.

Field Study

The field study element of MIST was added in Puget Sound and served as a great way to get a better understanding of the daily practices of information sharing from specific maritime industry perspectives. In Puget Sound and Honolulu the field study was comprised of only Facility Security Officers (FSO). In Delaware Bay the research team added a Vessel Security Officer (VSO) to the field study and the understanding of the private sector maritime perspective was noticeably expanded.

The steering committee and the AMSC Port Operations Board were very helpful in identifying the field study participants for MIST. They not only identified willing participants, but contacted them directly utilizing their personal relationships to facilitate participation. As we learned in MIST Honolulu, two researchers were present at each interview to provide a deeper understanding and diverse perspective.

Each interview was conducted in accordance to the process outlined in the Naval Postgraduate School human subjects' process. Interviews were conducted with a standardized question and answer period followed by a walking tour of operations to produce a greater understanding of a day in the life of this position. The interviews were recorded in written notes and a digital audio recording was made. Both written audio notes were transcribed for inclusion in the final report. Transcription was easier for this process as a result of lessons learned from Honolulu. As in Honolulu, Delaware Bay participants were provided with a Naval Postgraduate School coin as a token of appreciation and this act was well received and should be continued.

Recommendation

- Continue to expand to include additional perspectives from VSOs, agents, pilots and others

Workshop

Prior to the workshop, participants were provided with several polls to provide a baseline of perspectives and drive content. Based on lessons learned from prior MIST processes, these polls utilized NPS's Survey Monkey subscription and the questions were restructured and reworded for consistency. Survey Monkey proved to be a very useful tool. From the user perspective there were

[19] Fitting the Pieces Together- Improving Transportation Security Planning the Delaware Valley (March 2010),

[20] IBID

no complaints regarding the questions or use of the tool and from the research team perspective this tool facilitates quick analysis.

Recommendation

- Continue to leverage the NPS Survey Monkey subscription for future MIST polls.

The structure and design of the workshop has remained fairly consistent since the Puget Sound workshop design with the exception of revealing previous workshop results. It was thought that revealing the outcomes of the workshop of Los Angeles /Long Beach may have affected the responses in Puget Sound so in Honolulu the team used in-workshop polls to compare results of prior workshops to help provide trend data. This proved to be very cumbersome to facilitate as they were filled out at the end of the each section discussion and seemed rushed before breaks. In Delaware Bay, the in-workshop polls were filled out at the beginning of discussions which facilitated a much smoother flow of the workshop. However in the participant feedback there was a comment asking for the clarity between the ideas that came up from the workshop participants and the ideas that were raised by NPS based on what is done elsewhere. Further there was feedback regarding the evaluation categories to more traditional responses of very effective, marginally effective or not effective.

Recommendation

- Consider the influence of information provided from prior MIST processes in polls and facilitated discussion
- Re-work the polls to ensure the response categories are clear and relevant

MIST Puget Sound introduced the element of a keynote speaker. Honolulu was not as interested in keynote, but preferred to have a local leader kick off their MIST process. Their Captain of the Port (COPT), Barry Compagnoni provided a very inspirational keynote for MIST Honolulu. The steering committee for the Delaware Bay did discuss a keynote and thought it would be great to get the Department of Homeland Security Secretary Napolitano or a responder from the Aviation incident on the Hudson or a high level responder from Katrina. Unfortunately, due to the short time between the steering committee and the workshop, there was not time to secure an outside speaker. The USCG Sector Delaware Bay COPT Meredith Austin provided the keynote. Like CAPT Compagnoni, CAPT Austin is a graduate of the NPS Masters in Homeland Security program. She had just returned from a three month deployment to assist with the Deepwater Horizon. Her remarks provided a good jumping off point for the MIST process.

Recommendation

- Reconsider the use of a high-level keynote speaker as it does not really seem to add much benefit to the overall outcome

The workshop continues to provide a good balance of small and large group activities. The discussion after the small group activities demonstrates many ideas that would be more challenging to bring out in the larger activities. The organic conversations of the small groups are also very valuable in allowing quieter people to participate. The additional structure provided by preformatted flip charts was beneficial. The formatting of the flip chart pads facilitated more consistent sharing of small group outcomes.

Recommendation

- Rework flip charts by adding lines, changing the labels, and adding a comment section

As mentioned earlier, the wireless internet connection was sporadic making the small group activity of a Homeport usability test impossible. The team quickly recovered to facilitate the activity as a large group activity and the participants in that exercise were great, but it was not as effective. There was a lot of cross talk in the larger group and it was hard to hold the attention of the large group during times of thinking for the activity participants. This activity needs to be conducted in small groups to maximize the understanding and ensure the integrity of the outcomes.

Recommendation

- Provide static pages that can be used in the case of a technology failure

At the close of the first day, the MIST team met to review the day's outcomes and integrate the results into the slides for the kick off of the second day. This activity is very beneficial to demonstrate the amount of work that occurred the first day as well as set the stage for conversations of a way ahead. Due to the later start time of the MIST Delaware Bay at 0930, this activity pushed into the dinner hour and it seemed more challenging for the research team than in Honolulu. This was validated in typographical errors in the slides produced for day two. The one and a half day time frame still seems to be ideal to cover the content and gain the most participation. In addition, participants expressed a need for follow up meetings.

Recommendation

- Start at 0830 or 0900
- Hold a follow-up meeting to share results

The Way Forward

MIST is an interagency activity and we have been very fortunate to have participation and interest from many government agencies. The DOT/ MARAD and ODNI/GMAII provided us with fiscal support that greatly assisted in covering labor, securing supplies and printing services that supported this MIST. MIST Delaware Bay has begun to take the first step in taking this process to look at intermodal information sharing. Several Federal agencies provided participants to MIST workshops and we need to continue to capitalize on these relationships as well as socialize the outcomes of MIST activities to these agencies. MIST provides a very important analysis of information sharing at the local regional level. We provide a venue for Federal agencies to access the local and regional realities of interagency information sharing.

Recommendation

- Secure a consistent interagency sponsor to enable future MIST processes are executed with greater interagency vision

Appendix A: Methods

Using an iterative and participatory approach, the researchers partnered with federal, local and private sector stakeholders to assess the information sharing needs of regional maritime security personnel. The resulting research design included an issues workshop, field studies of port personnel, and participant email polling.

Purpose

The mission of MIST is *to create a process for interagency and international multilateral sharing of maritime threat information between private sector shipping and government agencies. This process must mitigate the concerns of private industry and provide value to both parties.*

Participant recruiting

Participants for the workshop and field study were invited to participate based on the recommendations of the local advisory committee. Participants included representatives from the following organizations:

Government

- DHS – Delaware Valley Intelligence Center (DVIC)
- DOT – MARAD
- Delaware Information and Analysis Center (DIAC)
- Delaware State Police
- Delaware Valley Regional Planning Commission (DVRPC)
- FBI – Baltimore Maritime Liaison Unit
- Information Sharing Environment
- New Jersey State Police
- Philadelphia Police Department
- U.S. Coast Guard Intelligence and Criminal Investigations
- U.S. Coast Guard Sector Delaware Bay

Industry

- Enterra Solutions, LLC
- Maritime Exchange of the Delaware River and Bay (MEX)
- Mariners Advisory Committee for the Bay and River Delaware (MAC)
- Norfolk Southern, Inc.
- TSA – Federal Air Marshal Service
- Sunoco, Inc.
- Vane Line Bunkering, Inc.
- Wilmington Tug, Inc.

Field study

There is significant literature that identifies key issues in the sharing of port security information between federal agencies. However, there is very little research about the daily practices of port personnel in the sharing of threat information. In this study, we sought to further the context of sharing threat information—specifically how, where, when, and why private sector personnel share threat information with the federal government. To support this we developed the following research questions:

1. What are the daily information sharing practices of port security personnel?
2. What are the social, psychological, operational, financial, and ideological factors that impact the sharing of threat information?

3. What are the barriers and constraints that exist in information sharing?
4. What are the opportunities to improve information sharing?

To explore the above research questions, we gathered examples of information sharing practices through ethnographic observation and qualitative interviews with selected Port personnel.

Workshop

The workshop was conducted over a day and a half and included large group discussions, breakout sessions, and a usability test. The workshop was segmented into several primary areas:

Tools for information sharing:

Participants were guided through a discussion of current tools, analyzed their usefulness, and then were introduced to a current and proposed tool for testing and evaluation.

Streamlining government requests:

In this section, we had participants identify, discuss, and rank government requests that were difficult. The participants used one dollar stickers to mark those items that they felt were the most important.

Incentives for information sharing:

Using a 360 degree value model, we had participants identify, discuss, and rank specific benefits that could be used to incentivize the private industry.

Models for Information Sharing:

This first new module on the second day of the workshop identified local best practice models, thoroughly evaluated those models, then allowed participants to brainstorm and define their collective ideal maritime threat information sharing model.

Next Steps:

The final activity for the workshop was to discuss how we could move forward.

Workshop slides

The slide presentation we used to structure the workshop is available upon request from the MIST team. Please contact Wendy Walsh – 831-917-5923 or wdwash@nps.edu.

Appendix B: Workshop Agenda

MIST Delaware River Workshop, 28-29 September 2010
WORKSHOP AGENDA

Tuesday, 28 September

0900 – 0930	**Registration /Networking**
0930 – 1000	**Introductions**
1000 – 1030	**Information Sharing**
1030 – 1045	**BREAK**
1045 – 1200	**Tools for Information Sharing**
1200 – 1300	**LUNCH**
1300 – 1400	**Streamlining**
1400 – 1430	**Collaboration**
1430 – 1445	**BREAK**
1445 – 1600	**Incentives**
1600 – 1630	**Multi-modal Issues**
1630	**DAY ONE WRAP**

Wednesday, 29 September

0900	**Check in / Networking**
0930 – 1045	**Models for Information Sharing**
1045 – 1100	**BREAK**
1100 – 1230	**Next Steps**
1230	**ADJOURN**

Appendix C: Polls and Evaluations

MIST Delaware Bay pre-workshop participant polls

Methodology

In preparation for the workshop, the MIST Delaware Bay participants were emailed a link to a poll designed and administered using Survey Monkey. Our goals were two-fold. First, we asked participants about key issues to help focus the design of the workshop. Second, we hoped that the questions would help participants focus on their needs in advance of the workshop. The consolidated poll results were incorporated into the final workshop presentation, and were integral in our preparation and facilitation.

Instrument

Following are the questions included in the pre-workshop poll. Results and analysis are included in the body of the report (*see **Detailed Findings***).

Introduction

> Welcome and thank you for agreeing to help us understand your perspectives on maritime security. The Maritime Information Sharing Taskforce (MIST) is a two-way process for understanding and communicating the needs of local, private sector communities when sharing maritime threat information with government stakeholders. As part of this process, we are holding a day and a half workshop on information sharing in your area. This poll is designed to help us understand what factors are most important to you locally. The information gathered here will be used to structure the workshop so your input is very important to us.
>
> The poll consists of ten questions and should take approximately 5 minutes. All answers will be kept anonymous.
>
> Thank you again for your help.

To help us better understand the wants and needs of different stakeholder groups, please tell us a little about yourself.

1. Your organization is a: (mark only one)
   Private company; Public association; Federal agency; Regional, State or local agency; Other, (please specify)

2. Your role in maritime security is: (mark only one)
   Facility Operations; Vessel Operations; Shipper; Law Enforcement; Intelligence; Port Authority; Other (please specify)

Please tell us what you think about information sharing.

3. When it comes to the sharing of threat information, your organization needs more information sharing between the public and private sector.
   Strongly Disagree; Disagree; Agree; Strongly agree; Comment (optional)

4. When it comes to maritime security, your organization needs more collaboration between the public and private sector.
   Strongly Disagree; Disagree; Agree; Strongly agree; Comment (optional)

Please take a moment to help us identify maritime security information sharing issues of interest in your region.

5. In your daily work, what are your three most pressing problems with sharing information? (select only three)

   Access to information; Timeliness of information; Accuracy/Reliability of information; Usability of information (Is it relevant and actionable?); Information overload; Reporting procedures; Other (please specify)

6. What is the most important issue that you would like to discuss during the upcoming workshop on maritime security? (Please provide detail)

7. At the workshop, we will analyze a specific information sharing tool for its effectiveness. What tool would you like to target for discussion?

   HOMEPORT (USCG); MarView (MARAD); Regional Information Sharing Systems Program-RISS ATIX (DOJ); Other (please specify)

Please tell us about the maritime security information sharing resources in your region.

8. What organizations or meetings do you find most useful when working in maritime security? (Include things like associations, agencies, special interest groups, local events, conferences and workshops)

9. Why are these organizations important?

10. What tools do you find most useful when working in maritime security? (Include things like web sites, data analysis software, communication and situational awareness tools)

In-session workshop polls

Methodology

This series of four polls was administered at strategic points throughout the day and a half workshop to solicit feedback on issues that may not have surfaced during large and small group discussion, but were discussed at workshops in other regions. By collecting feedback on common issues, we hope to allow comparative analysis of findings from a variety of regions.

Instruments

These six polls were included in the participants packets distributed at the start of the workshop on day one, each on a separate page. The pages were labeled R1 thru R30 to protect anonymity while grouping responses by participant. Results and analysis of the workshop polls are included in the full report (see ***Detailed Findings***).

POLL 1: Tell us about yourself...

1. Your organization is a: (mark only one)

   Private company; Public association; Federal agency; Regional, State or local agency; Other, (please specify)

2. Your role in maritime security is: (mark only one)

   Facility Operations; Vessel Operations; Shipper; Law Enforcement; Intelligence; Port Authority; Other (please specify)

POLL 2: What type of maritime security information is most important to you?

Please look at the entire list below. Then indicate the relative importance to you of the following types of information (7 point scale, most to least)

General threats to facilities or vessels; Specific threats to my or nearby company, facility, or ship; Details of specific threats; Risk mitigation; Impacts on traffic and movement of goods; The safety of the workforce; Past terrorist incidents; Follow-up reports of specific threats; Response plans; Risk or vulnerability assessments; Other (please specify)

POLL 3: How can interactions with government be streamlined?

Please look at the entire list below. Then indicate the relative importance to you of the following types of recommended government improvements (7 point scale, most to least)

Improve information sharing between government agencies; Improve coordination and sequencing of government regulations; Simplify government processes and programs; Provide a single threat reporting system; Provide a central contact for information distribution; Provide a single place to access threat information; Strip unclassified information from classified; Standardize processes such as log-ins and data types; Other (please specify)

POLL 4: How can industry and government collaboration be improved?

Please look at the entire list below. Then indicate the relative importance to you of the following types of collaboration (7 point scale, most to least)

Provide better information TO the private sector; Provide information that is useful; Align government policies and governance structures ; Increase coordination between federal, state and local agencies; Increase coordination between industry partners; Increase trust; Minimize jurisdiction wars and the misuse of power; Reduce fears of retribution (targeting, stricter standards, blame); Increase face-to-face communication; Other (please specify)

POLL 5: What incentives are most effective?

Please look at the entire list below. Then indicate the relative importance to you of the following types of incentives for sharing information (7 point scale, most to least)

Fewer costs incurred; Quicker business resumption after an event; Workplace satisfaction; Improved customer service; Improved decision making; Personal pride of work, professionalism; Improved business logistics; More efficient supply chain; Protection of assets; Positive public opinion; Environmental stewardship; Greater certainty and reliability; Increased port use ; Faster vessel turnaround; Personal financial rewards; Other (please specify)

POLL 6: What are your biggest security challenges?

Please look at the entire list below. Then indicate the relative importance to you of the following maritime security challenges (7 point scale, most to least)

Access controls and barriers, fences, guards and surveillance equipment; Shipping, trucking and rail connections; Cargo inspections; Data management; Military and law enforcement readiness and response capabilities; Passenger vessels (ferries, *cruise ships, personal watercraft); Cargo theft; Planning for disaster recovery and continuity of business; International issues; Other (please specify)*

MIST Delaware Bay Workshop evaluation

On the second day of the MIST Delaware Bay workshop, attendees were sent an email link to the MIST Delaware Bay Workshop evaluation on Survey Monkey. Participants were encouraged to complete this evaluation before the end of the week of the workshop. After one week only five participants had completed the survey, so an email reminder was sent. At the time of analysis we had twelve responses. Results and analysis of the workshop evaluation is included in the full report (see ***Lessons Learned***).

Thank you for participating in the MIST workshop. Please take a moment to evaluate your experience.

Overall, what are your thoughts on this workshop? (*Not at all, Not very, Somewhat, or Very)*

How well organized was this workshop?
How useful was this workshop?
How effective was the workshop in identifying issues with sharing information?

How appropriate were the topics we discussed? (check all that apply) *(Personally interesting, Applicable to my job, or Not applicable)*

Incentives for the private sector
Streamlining government requests
Tools for information sharing
Private sector issues in information sharing
Solutions for better information sharing
Networking

Were the right people in attendance?

Yes or No

Please provide us feedback on the length and pacing of the workshop. *(Not enough, Just right, or Too much)*

The length was:
The speed was:
The number of breaks was:

The workshop was: *(Disagree, Somewhat disagree, Somewhat agree, or Agree)*

Too long
Too short
Made me feel rushed
Was too slow
Didn’t provide enough breaks

Are there any other comments you would like to share with us about your experience with MIST?

Follow up poll

Methodology

Sent one month after the workshop event, this piece was designed to solicit considered feedback on our process and topics covered after participants had time to reflect.

Instrument

Thank you for participating in the recent MIST workshop in your region. Now that a month has passed, please take the opportunity to share any issues that surfaced for you following our day and a half workshop. Thank you for your time and input.

For you, the most important issue discussed in the recent workshop was: (select one)

- □ Coordination, communication, and streamlining
- □ Incentives for threat information sharing
- □ Partner organizations, agencies, and associations
- □ Best practices, ideal system design
- □ Other (please specify)

How likely would it be that you would recommend MIST to a colleague?

As we prepare to bring the MIST process to other regions, it would help us to know what you found most useful. Please share your thoughts:

Are there any other comments you would like to share about your recent experience with MIST?

Appendix D: Acronyms and Definitions

AIS	Authorized Identification System
AMSC	Area Maritime Security Committee
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
CBP	Customs and Border Protection
COTP	Captain of the Port
DHS	U.S. Department of Homeland Security
DIAC	Delaware Intelligence and Analysis Center (fusion center)
DoD	Department of Defense
DON	Department of the Navy
DOT	Department of Transportation
DVIC	Delaware Valley Intelligence Center (fusion center)
DVRPC	Delaware Valley Regional Planning Commission
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FAA	Federal Aviation Administration
FIST-FIG	Field Intelligence Support Team (USCG)
FSO	facility security officer
GMAII	Global Maritime and Air Intelligence Integration
GMISS	Global Maritime Information Sharing Symposium
GPS	global positioning system
HIDTA	High Intensity Drug Trafficking Areas program
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
LA/LB	Los Angeles/Long Beach
MAC	Mariners Advisory Committee for the River and Bay Delaware
MARAD	Maritime Administration (DOT)
MCAC	Maryland Criminal Intelligence Center (fusion center)
MDA	maritime domain awareness
MDSRP	Maritime Defense and Security Research Program (NPS)
MEX	Maritime Exchange for the Delaware River and Bay
MISNA	Maritime Information Services of North America
MIST	Maritime Information Sharing Taskforce
MPO	Metropolitan Planning Organization
NMCO	National Maritime Domain Awareness Coordination Office
NMIC	National Maritime Intelligence Center
NPS	Naval Post Graduate School
NRC	National Reporting Center
NSMS	National Strategy for Maritime Security
ODNI	Office of the Director of National Intelligence
PaCIC	Pennsylvania Criminal Intelligence Center (fusion center)
PCII	protected critical infrastructure information
PHMSA	Pipeline and Hazardous Materials Safety Administration (DOT)
ROIC	Regional Operations Intelligence Center (New Jersey fusion center)
TSA	Transportation Security Administration
TWIC™	Transportation Worker Identification Credential
USCG	U.S. Coast Guard
USDA	U.S. Department of Agriculture
VIPR	Visible Intermodal Prevention and Response

DEFINITIONS:

Maritime Domain Awareness: as defined in the 2005 National Strategy for Maritime Security: National Plan to Achieve Maritime Domain Awareness, "*Maritime Domain Awareness (MDA)* is the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States. MDA is a key component of an active, layered maritime defense in depth. It will be achieved by improving our ability to collect, fuse, analyze, display, and disseminate actionable information and intelligence to operational commanders." http://www.dhs.gov/xlibrary/assets/HSPD_MDAPlan.pdf

Maritime domain awareness is intended to enable the early identification of potential threats and enhance appropriate responses, including interdiction at an optimal distance with capable prevention forces. Achieving awareness of the maritime domain is challenging. The vastness of the oceans, the increase in commercial and recreational vessel traffic, continued ocean and inland water research being performed from vessels, and the operation of U.S. military vessel traffic has placed burdens on waterway and port safety and security services, and raised the risk of accidents. The challenge is to ensure that the business, recreational, safety, military, and security needs of vessels on our oceans, harbors, ports, and inland waterways are met. Security mandates including the Maritime Transportation Security Act of 2002 and the Safe Port Act of 2006, among other legislative initiatives, have created additional pressures on the MTS to balance operational requirements and security needs with limited public and private resources.

Protecting a port and monitoring miles of continuous activity along the waterway involves a lot of diverse technology. Some of that technology is new and evolving and being mixed in with standard and reliable tools for intrusion detection and rapid response. The most critical factor for MDA is ensuring that all of the technology works together on a common operating platform and in real time to be effective both in protecting critical infrastructure and in alerting first responders, property owners, and law enforcement, including the US Coast Guard. Building a common operating platform is neither easy nor cheap. MoUs need to be developed and, in tough economic times, responsibilities are often cross-jurisdictional and complicated. Chemical detection sensors are designed to detect more than 15 different toxic industrial chemicals and 7 or more chemical warfare agents. Radiation detectors are used in limited situations. But, using this technology as an example, it is unclear how, if at all, the responsibilities between EPA, State DEPs, USCG, and the private chemical industries are actually coordinated. Further, underwater sonar systems/radar and thermal short-range and long-range cameras add a level of complexity and serve as additional technology tools to be used by private port owners and law enforcement personnel. Once installed, these tools will be available to verify the legitimacy of any e-mail alerts. We need to routinely prioritize the most critical sites, identify available tools/investments along with the acceptable level of port partner responsibilities considering scarce resources, and work together to achieve MDA.

Appendix E: Regional Resources Catalog

The following list of regional resources includes:

- Fusion centers
- Private sector organizations
- Local and state government agencies
- Transportation agencies
- Taskforces, working groups, programs and councils
- Regional alert services
- Federal level resources
- and Training providers

This list is not meant to be exhaustive, but provide a survey of regional resources available for sharing maritime security threat information.

REGIONAL FUSION CENTERS

Delaware Valley Intelligence Center (DVIC)

- The DVIC will be a 24/7 operation staffed by member agencies. An "all hazards, all crime" operation, the DVIC will provide comprehensive information sharing to the Delaware Valley region, a four state area of responsibility.

Delaware Information and Analysis Center (DIAC)

- The Delaware Information and Analysis Center is an “All Crimes, All Hazards” approach to Homeland Security at the state level. DIAC provides real time information and intelligence to the Law Enforcement sector.

Maryland Criminal Intelligence Center (MCAC)

- The Maryland Coordination and Analysis Center is an umbrella organization of local, state and federal agencies, as well as representatives from the private sector, that coordinates activities, develops policy, and implements strategic plans to combat terrorism in the State of Maryland.

New Jersey Regional Operations Intelligence Center (ROIC)

- The New Jersey Regional Operations Intelligence Center is an “all-crimes, all-threats, all-hazards” fusion center that supports law enforcement and homeland security agencies across New Jersey.

Pennsylvania Criminal Intelligence Center (PaCIC)

- The Pennsylvania Criminal Intelligence Center provides law enforcement agencies throughout the Commonwealth with one central point of contact for intelligence information, investigative data, and public source information.

PRIVATE SECTOR ORGANIZATIONS

Association of Contingency Planners, Liberty Valley Chapter – Philadelphia

http://libertyvalley.acp-international.com/

- A professional organization that provides a forum for the exchange of experiences and information for business continuity leaders.

Center City District

http://www.centercityphila.org/about/Crime.php

- A coalition of business leaders who work to reduce and prevent crime and to enhance the perception of safety in Philadelphia.

Philadelphia Crime Prevention Council of the City Center District

- A forum for federal, state and local law enforcement officials and corporate security professionals from the retail, office, banking, hospital, hotel and utility sectors. The forum discusses current crime trends, emergency preparedness, terrorism and other matters of common concern and to develop coordinated strategies to combat crime.

Maritime Exchange of the Delaware River and Bay (MEX)

http://www.maritimedelriv.com/

- In continuous operation since 1875, the not-for-profit trade association the Maritime Exchange for the Delaware River and Bay is dedicated to promoting and encouraging commerce on the Delaware River and Bay.

Mariners Advisory Committee (MAC)

http://www.macdelriv.org

- Comprised of Master Mariners and River Pilots, the MAC focus is on safety of navigation, particularly large ocean-going vessels.

LOCAL AND STATE GOVERNMENT AGENCIES

FBI Philadelphia Joint Terrorism Task Force (JTTF)

http://philadelphia.fbi.gov/partners.htm

- The Philadelphia Division of the FBI has three Joint Terrorism Task Forces that bring together representatives of local, state, and federal agencies.

Managing Director's Office of Emergency Management (MDO-OEM)

http://oem.readyphiladelphia.org

- The Managing Director's Office of Emergency Management (MDO-OEM) is responsible for ensuring the readiness of the City of Philadelphia.

New Jersey Office of Homeland Security and Preparedness (NJ OHSP)

http://www.state.nj.us/njhomelandsecurity

- With an all-hazards approach, the mission of the NJ OHSP is to administer, coordinate, lead, and supervise New Jersey's counterterrorism and preparedness efforts. NJ OHSP is also tasked with coordinating the emergency response efforts across all levels of government, law enforcement, emergency management, nonprofit organizations, other jurisdictions, and the private sector.

Pennsylvania Emergency Management Agency (PEMA)

http://www.pema.state.pa.us

- PEMA's mission is to coordinate state agency response, including the Office of the State Fire Commissioner and Office of Homeland Security, to support county and local governments in the areas of civil defense, disaster mitigation and preparedness, planning, and response to and recovery from man-made or natural disasters.

Pennsylvania Office of Homeland Security and Preparedness (PA OHSP)

http://www.homelandsecurity.state.pa.us

- The Pennsylvania Office of Homeland Security is a Commonwealth office within the Pennsylvania Emergency Management Agency (PEMA).

TRANSPORTATION

Delaware River and Bay Authority (DRBA)

http://www.drba.net/Home.aspx

- The DRBA, overseen by six commissioners from New Jersey and six from Delaware, is charged with providing vital transportation links between the two states as well as economic development in Delaware and the four southern counties of New Jersey.

Delaware River Port Authority (DRPA)

http://www.drpa.org/

- The Delaware River Port Authority of Pennsylvania and New Jersey is a regional transportation agency serving Southeastern Pennsylvania and Southern New Jersey.

Delaware Valley Regional Planning Commission (DVRPC)

http://www.dvrpc.org/

- Serving a nine county region, DVRPC is dedicated to uniting the region's elected officials, planning professionals to build consensus on improving transportation, promoting smart growth, protecting the environment and enhancing the economy.

New Jersey Department of Transportation (NJ DOT)

http://www.state.nj.us/transportation/

- NJ DOT's mission is to provide reliable, environmentally and socially responsible transportation and motor vehicle networks and services to support and improve the safety and mobility of people and goods in New Jersey.

NJ TRANSIT

http://www.njtransit.com

- NJ TRANSIT is New Jersey's public transportation corporation. Covering a service area of 5,325 square miles, NJ TRANSIT is the nation's third largest provider of bus, rail and light rail transit, linking major points in New Jersey, New York and Philadelphia.

Pennsylvania Department of Transportation (Penn DOT)

http://www.dot.state.pa.us/

- Penn DOT provides services and a safe intermodal transportation system, and operates and maintains the commonwealth's highway and bridge infrastructure.

Philadelphia Regional Port Authority (PRPA)

http://www.philaport.com/

- The Philadelphia Regional Port Authority (PRPA) is an independent agency of the Commonwealth of Pennsylvania charged with the management, maintenance, marketing, and promotion of publicly owned port facilities along the Delaware River in Philadelphia. The PRPA operates seven terminals along the Delaware River within the city of Philadelphia. The sites also have rail connections to CP Rail System, CSX, and Norfolk Southern.

Port Authority Transit Corporation (PATCO)

http://www.ridepatco.org/

- PATCO a total of 13 intermodal transportation stations, and manages total parking is available for over 12,000 cars daily at 7 stations.

Southeast Pennsylvania Transportation Authority (SEPTA)

http://www.septa.org/

- Serving Bucks, Chester, Delaware, Montgomery, and Philadelphia Counties, SEPTA is comprised of buses, subways, trolleys, trackless trolleys, high speed rail and commuter trains - commonly referred to as Regional Rail.

TASKFORCES, WORKING GROUPS AND COUNCILS

Area Maritime Security Council (AMSC) Sector Delaware Bay

http://www.uscg.mil/d5/sectDelawareBay/ ***USCG Sector Delaware Bay 215-271-4800***

- The Area Maritime Security Committee (AMSC) for USCG Sector Delaware Bay is a partnership of federal, state and local law enforcement and intelligence organizations; governmental, regulatory, public safety and emergency management agencies; organized labor; commercial and recreational waterway users; and, public and private sector stakeholders who are committed to improving the security of the maritime transportation system in the USCG Sector Delaware Bay area of responsibility (AOR).

Philadelphia Area Regional Transit Security Working Group (PARTSWG)

- Working to develop a regional information sharing plan for a terror attack with an Improvised Explosive Device (IED) against the rail system in Philadelphia, the PARTSWG members include Amtrak, NJ Transit, Pennsylvania Emergency Management Agency (PEMA), the Philadelphia Police Department, the Port Authority Transit Corporation (PATCO), the Southeastern Pennsylvania Transportation Authority (SEPTA), the Pennsylvania Department of Transportation (Penn DOT), the NJ Department of Transportation (NJ DOT), the Delaware River Port Authority (DRPA), and the Delaware River and Bay Authority (DRBA).

Southeastern Pennsylvania Regional Task Force (SEPA RTF)

http://www.sepatransportation.com/default.aspx

- The Southeastern Pennsylvania Regional Task Force, in conjunction with PEMA and DVRPC, has undertaken creation of the Southeastern Pennsylvania Emergency Transportation Plan to ensure an appropriate and consistent response to events impacting the five country area. The SEPA RTF is comprised of the City of Philadelphia, as well as the counties of Bucks, Chester, Delaware, and Montgomery, operating in an area defined as the Urban Area Security Initiative (UASI).

FEDERAL RESOURCES

Department of Transportation Maritime Administration (DOT – MARAD)

http://www.marad.dot.gov ***1-800-99-MARAD or pao.marad@dot.gov***

- MARAD is the agency within the U.S. Department of Transportation dealing with waterborne transportation; and works in many areas involving ships and shipping, shipbuilding, port operations, vessel operations, national security, environment, and safety. MARAD is also charged with maintaining the health of the merchant marine, and maintains a fleet of cargo ships in reserve to provide surge sealift during war and national emergencies.

National Maritime Intelligence Center (NMIC)

http://www.nmic.gov/

- In January 2009, the Director of National Intelligence (DNI) established the National Maritime Intelligence Center (NMIC) to integrate and optimize the Global Maritime Community of Interest's

(GMCOI) efforts to achieve and maintain holistic Maritime Domain Awareness. The GMCOI includes federal, state, local, tribal, and territorial partners; as well as international partners, maritime industry, and academia. The NMIC works to close analytic and collection gaps, deliver interagency collaboration and information sharing solutions, advise interagency policy development, and research and evaluate emerging technologies. The NMIC neither collects nor produces intelligence. It breaks down barriers and creates enabling structures and cultures so the GMCOI can perform these functions optimally.

National Maritime Domain Awareness Coordination Office (NMCO)

http://www.gmsa.gov/

- The mission of the NMCO is to facilitate the creation of a collaborative global, maritime, information sharing environment through unity of effort across entities with maritime interests. In order to achieve Global Maritime Situational Awareness, NMCO works with global partners to increase the discoverability and share-ability of information relevant to those engaged in managing the security, safety, environment and commerce associated with the maritime domain.

U.S. Coast Guard National Headquarters

http://www.uscg.mil/

- The U.S. Coast Guard is one of the five armed forces of the United States and the only military organization within the Department of Homeland Security. The Coast Guard protects the maritime economy and the environment, defends our maritime borders, and saves those in peril.

Information Sharing Environment (ISE)

http://www.ise.gov

- The primary focus of the ISE is any mission process, anywhere, which has a material impact on detecting, preventing, disrupting, responding to, or mitigating terrorist activity. End-to-end mission processes are operated by ISE mission partners and directly support frontline law enforcement, public safety, homeland security, intelligence, defense, and diplomatic personnel. They encompass a broad range of activities and include processes that support alerts and notifications; suspicious activity report gathering, vetting, and sharing; terrorist watch list maintenance and use; and other activities and processes with direct mission impact.

TOOLS

Homeport

http://homeport.uscg.mil ***USCG Sector Delaware Bay 215-271-4800***

- Homeport is the United States Coast Guard's enterprise internet portal for the Maritime Community. Homeport's secure, role-based environment brings together US Coast Guard personnel, members of the Maritime Community, and other designated individuals allowing them to share information quickly. In addition, Maritime Community members can receive pertinent information from the Coast Guard, submit and edit security plans or vessel response plans, and collaborate in user specific communities.

MarView

www.marview.gov ***1-866-466-5221 or 202-385-HELP or ServiceDesk@dot.gov***

- The U.S. Department of Transportation Maritime Administration is the proud owner of MarView, an integrated data-driven environment providing essential information to support the strategic requirement of the U.S. Marine Transportation System (MTS) and its contribution to the economic viability of the Nation. MarView provides the ability to fuse data together to create models and simulations for capacity planning, economic impact analysis, on-demand forecasting, plans for mitigating and reacting to emergency situations. Information available to registered stakeholders on a tiered security level system.

Maritime Domain Awareness Information Portal

www.mda.gov

- A single access point to U.S. government maritime-related information for members of the Global Maritime Community of Interest. Established by aligned federal partners (DOT-MARAD, NMIC, GSA, ONI) to facilitate an integrated interagency effort to produce and disseminate Maritime Domain Awareness across the whole of government and to ensure productive exchange with our state, local, tribal, business and industry, and international partners. NMIC worked closely with GSA and DOT Maritime Administration personnel to ensure the domain's completion and is currently working with ONI to formally establish the site.

All Partners Access Network (APAN)

http://community.apan.org/

- All Partners Access Network (APAN) is a "community of communities" web site that combines the benefits of unstructured collaboration (wikis, blogs, forums) and structured collaboration (file sharing, calendar) with the personalization of social networking to facilitate unclassified information sharing with multinational partners, non-governmental organizations, and among various US Federal and State agencies. Currently, APAN hosts five Maritime Domain Awareness communities.

RISS

http://www.riss.net/

- Regional Information Sharing Systems (RISS) is a federally funded program to support regional law enforcement efforts in combating crimes of all types. The mission of RISS is to support law enforcement efforts nationwide to combat illegal drug trafficking, identity theft, human trafficking, violent crime, terrorist activity, and to promote officer safety. Today, RISS is a national network comprised of six multistate centers designed to operate on a regional basis.

REGIONAL ALERT SERVICES

There are several services available in this region for hazard and alert notifications. This list is not intended to be inclusive of all alert services available, only to give a sample of the offerings:

AlertPA ***https://alert.pa.gov***	Pennsylvania uses AlertPA to deliver emergency and weather alerts, health notifications, tax notifications, and updates to citizens and partners
Alert Philadelphia ***https://www.alertphila.com***	A system to deliver emergency alerts designed specifically for businesses, law enforcement and first responders coordinated by the Philadelphia Police Department and Center City District. *NOTE: users of Alert Philadelphia automatically receive Ready Notify PA emergency alerts for Philadelphia*
Ready Notify PA ***http://www.readynotifypa.org/*** ***https://phila.alertpa.org***	A service of the Southeastern Pennsylvania Regional Task Force to send emergency text alerts and other important notifications
Ready PA ***http://www.readypa.org***	A monthly update from the Philadelphia Office of Emergency Management

TRAINING PROVIDERS

Please note that this list is not meant to be an exhaustive listing of regional training providers, only a sample of what is available.

Delaware County Emergency Training Center

http://www.delcoestc.org/

- The training center, formally known as the Folcroft Incinerator Facility is located on Calcon Hook Road in Darby Township, Delaware County Pennsylvania. Courses available in emergency response, CERT, hazardous materials handling, fire response and suppression, emergency vehicle operations, and more

Managing Director's Office of Emergency Management (MDO-OEM)

http://oem.readyphiladelphia.org

- The Managing Director's Office of Emergency Management (MDO-OEM) works with local, regional, state, and federal partners to conduct preparedness exercises. These exercises serve to test plans, reinforce response and management techniques, identify areas for improvement, and promote better interagency coordination and cooperation. MDO-OEM also provides training to city and partner agencies.

Pennsylvania Emergency Management Agency (PEMA)

http://www.pema.state.pa.us

- PEMA manages the Bureau of Training, Exercise and Evaluation to provide innovative and professional training to state and local emergency management personnel, elected and appointed officials, emergency responders, members of volunteer organizations active in disasters and other professionals who prepare for and respond to emergencies. The division provides public education, professional development training, and technical training to public safety volunteers from state government and local communities across the commonwealth and conducts all hazards related exercises to test preparedness of state agencies, local governments, community public service organizations i.e. schools, hospitals, and others. We also administer a statewide Emergency Exercise Program and oversee the Pennsylvania Emergency Management Coordinator certification program.

U.S. Coast Guard Sector Delaware Bay

http://www.uscg.mil/d5/sectDelawareBay/

- The U.S. Coast Guard offers a variety of trainings throughout the year to a wide sector of the maritime community. Those on the AMSC distribution list receive notification of locally available training opportunities. One such offering is *Boarding Team 101*, held annually by the Vessel Boarding Security Team at Coast Guard Sector Delaware Bay. In this course Coast Guard members learn law enforcement fundamentals to operate as a boarding team member on the water.

Department of Transportation Maritime Administration (DOT – MARAD)

http://www.marad.dot.gov 1-800-99-MARAD or pao.marad@dot.gov

- Beyond operating the U.S. Merchant Marine Academy at Kings Point, New York, MARAD also supports continuing education for current mariners. MARAD has also developed guidelines and curricula for security training for a variety of people who work around ports and ships.

Current MARAD training offerings are listed online:
http://www.marad.dot.gov/documents/MTSA_Updated_list_of_MTSA_certified_courses_SB_Correct-9-30-10.pdf

Appendix F: References

Delaware Valley Regional Planning Commission (2010). "Fitting the Pieces Together: improving transportation security planning in the Delaware Valley." March 2010. Last accessed 22 October 2010 at http://www.dvrpc.org/reports/09018.pdf

DHS (November 2010). "Guarding Against Terrorism and Ensuring Transportation Security." *Progress in Implementing 9/11 Commission Recommendations: July 2010 Update*. Last accessed 16 November 2010 at http://www.dhs.gov/xlibrary/assets/9-11-commission-update-report-7-22-10.pdf

DHS (July 2010). "Secretary Napolitano Announces Rail Security Enhancements, Launches Expansion of "See Something, Say Something" Campaign." *DHS press release* 1 July 2010. Last accessed 16 November 2010 at http://www.dhs.gov/ynews/releases/pr_1278023105905.shtm

GAO (2010). GAO-10-435R: Intermodal Transportation Facilities, report released 27 May 2010.

GAO (2007). "Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers" *GAO-08-35*, August 2007. Last accessed 5 November 2010 at http://www.gao.gov/new.items/d0835.pdf

Hughes, E. and L.M. Roszkowski, E. Thompson (2009). "The National Infrastructure Protection Plan: A Resilient America Through Partnership Innovation" USCG Proceedings, Spring 2009 p. 50. Last accessed 9 November 2010 at http://www.uscg.mil/proceedings/spring2009/articles/50_Hughes,%20Roszkowski,%20Thompson_National%20Infrastructure%20Protection%20Plan.pdf

Ives, P. and P. Randall (1997). "Success Story: prevention through people, circa 1964." *USCG Proceedings of the Marine Safety Council*, July-September 1997, pp 44-47.

Salem, Anita with Wendy Walsh and Owen Dougherty (2008). "Industry and Public Sector Cooperation for Information Sharing: Ports of Long Beach and Los Angeles," a joint publication of the *Naval Postgraduate School* and the *Maritime Administration*. September 2008. Last accessed 29 January 2010 at http://www.gmsa.gov/gmiss

Salem, Anita with Wendy Walsh and Lyla Englehorn (2009). "Industry and Public Sector Cooperation for Information Sharing: Ports of the Puget Sound," a publication of the *Naval Postgraduate School*. July 2009. Last accessed 29 January 2010 at http://www.gmsa.gov/gmiss

TSA (June 2007). "VIPR Teams Enhance Security at Major Local Transportation Facilities" TSA website article published 20 June 2007. Last accessed 5 November 2010 at http://www.tsa.gov/press/happenings/vipr_blockisland.shtm

TSA (August 2007). “Building Security Force Multipliers” TSA website article published 12 August 2007. Last accessed 9 November 2010 at http://www.tsa.gov/what_we_do/tsnm/mass_transit/force_multipliers.shtm

TSA TSSP (2007). Transportation Systems Sector-Specific Plan (TSSP), released May 2007. Last accessed 1 November 2010 at http://www.tsa.gov/assets/pdf/transportation_base_plan_appendixes.pdf